Lebanese FinTech BDL Compliance Guide

A Comprehensive Public Reference for Regulatory Compliance Mapping

Version: 1.0

August 25, 2025

Target Audience: Lebanese FinTech companies, compliance officers, security professionals, legal teams, auditors, and consultants

Purpose: Public reference guide for understanding and implementing Banque Du Liban (BDL) regulatory compliance requirements

Scope and Applicability: This guide focuses primarily on the regulatory requirements issued by the Banque du Liban that impact the technology, data, and operational frameworks of regulated financial institutions. Applicability to a specific FinTech entity depends on its licensing status. Non-bank FinTechs (e.g., Payment Service Providers, technology service providers) often fall under these obligations contractually when partnering with a BDL-supervised institution. It is not an exhaustive guide to all corporate or employment laws in Lebanon. Always consult with qualified legal counsel to determine the precise obligations for your specific business model.

Author: Abed Al Rahman Naboulsi - Information Security Officer, Capital Outsourcing SAL

Table of Contents

1. Executive Summary

This guide provides Lebanese FinTech companies with a comprehensive framework for understanding and implementing Banque Du Liban (BDL) regulatory compliance requirements. It includes practical mapping between BDL regulations and international standards (ISO 27001:2022, ISO 27017, PCI DSS, Basel III) to help organizations achieve regulatory compliance while working with hosting providers.

1.2 🚨 Key Regulatory Reality

While Banque Du Liban (BDL) has not issued a standalone circular explicitly prohibiting all forms of cloud computing, its stringent data sovereignty requirements, coupled with the provisions of the Banking Secrecy Law and BDL's supervisory oversight, effectively mandate that all sensitive financial data for regulated activities must remain within Lebanese jurisdiction. This practical reality leads to an effective prohibition of international cloud-based solutions (like AWS, Azure, GCP) for production data and core regulated activities. [1]

1.3 ⚠ Most Critical BDL Requirements & Strict Prohibitions

1.3.1 EFFECTIVELY PROHIBITED ✗

- **Hosting of production data subject to Banking Secrecy Law on international public clouds (e.g., AWS, Azure, GCP).** This is due to BDL's strict data sovereignty, supervisory access, and banking secrecy requirements, making such hosting non-viable without explicit **BDL approval** under a future framework.
- **Cross-border export of banking-secrecy-protected data without an explicit legal basis and supervisory approval (mere client consent is not sufficient)**
- **Outsourcing of compliance monitoring** to third parties. Circular 128 does not, by itself, prohibit outsourcing technology, infrastructure, hosting, managed security operations, or other IT/operational services, provided the institution maintains an in-house, independent Compliance Department and retains overall accountability.

- **Uncontrolled remote access from outside Lebanon to production systems.** Any such access must be considered exceptional, justified by a formal risk assessment, and implemented with robust compensating controls (e.g., Privileged Access Management, session recording, multi-factor authentication, geo-fencing, and time-bound approvals), subject to BDL/BCC review.
- **Data processing outside Lebanese territory**
- **Backup replication** to foreign data centers

1.3.2 MANDATORY REQUIREMENTS ☑

- **Prior BDL approval** for all digital banking applications
- **Prompt incident reporting to BDL for critical security incidents (generally interpreted as within 24 hours of confirmation).** Note that the Special Investigation Commission (SIC) must also be notified in cases involving suspicious financial transactions or money laundering.
- **Two-Factor Authentication (2FA):** Mandatory for all interactive user access to critical systems, all administrative/privileged accounts, and all remote access sessions. A risk-based approach may be documented for low-risk, internal-only systems.
- **Board-approved business continuity plans** submitted to BCC
- **Lebanese jurisdiction** for all data and infrastructure
- **Strong encryption** for all data in transit (e.g., TLS 1.2+) and at rest (e.g., AES-256)

2 BDL Regulatory Framework Overview

2.1 Primary BDL Regulations for FinTech

2.1.1 BDL Basic Circular 69/2000 - Electronic Banking Operations

- **Requirement:** Prior BDL approval for all digital banking applications
- **Impact:** Must demonstrate compliance before launching services
- **Documentation:** Technology infrastructure assessment required

2.1.2 BDL Basic Circular 144/2017 - Cybersecurity Measures

- **Requirements:**
    - Two-factor authentication mandatory
    - Strong encryption in transit (TLS 1.2/1.3) and encryption at rest (e.g., AES-256). Where feasible, apply application-layer encryption for the most sensitive data.
    - 24-hour incident reporting to BDL
    - Regular security assessments and penetration testing

2.1.3 BDL Basic Circular 141/2017 - Recovery Plans

- **Requirements:**
    - Board-approved business continuity plans
    - Plans submitted to Banking Control Commission (BCC)
    - Regular testing and updates
    - Alternative site operations within Lebanon

2.1.4 BDL Basic Circular 128/2013 — Scope of Restriction

- **Key Restrictions under Circular 128:**
    - Compliance monitoring cannot be outsourced (Article 11).
        - **Clarification:** Circular 128 does not, by itself, prohibit outsourcing technology, infrastructure, hosting, managed security operations, or other IT/operational services, provided the institution maintains an

in-house, independent Compliance Department and retains overall accountability.

- BDL must have supervisory access to all systems
- Exit strategies must be documented

2.1.5 Banking Secrecy Law of 1956

- **Critical Requirements:**
  - Client confidentiality (with significant legal exceptions introduced by recent amendments). [2][3]
  - **Key Amendments (Law No. 306/2022, and further in 2025)** now permit authorized bodies (judiciary, tax authorities, BDL, BCC, and appointed auditors) to access banking records to investigate corruption, conduct audits, and ensure financial transparency. [2][4]
  - Data containing client information cannot leave Lebanese territory without a proper legal framework.
  - Criminal penalties for unauthorized disclosure remain.
  - **Effect:** Despite amendments, the need for local oversight and the law's remaining confidentiality obligations still effectively prohibit international cloud hosting for sensitive financial data.

3 Detailed BDL Circular Analysis

3.1 🏛 BDL Basic Circular 69/2000 - Electronic Banking Operations

*3.1.1 **Scope and Application***

Issued on **March 30, 2000**, this circular establishes the foundational rules for electronic banking and financial operations in Lebanon. [8][9] It requires institutions to get prior BDL approval before launching electronic services, ensure data protection, and facilitate BDL's supervisory access. [9][10] It has been amended by several intermediate circulars over the years to address new technologies and AML/CFT requirements. [11]

Reference Link:

https://www.bdl.gov.lb/CB%20Com/Laws%20And%20Regulations/Basic%20Circulars/Decision_7548_EN%C2%A782_3.pdf [9]

*3.1.2 **Key Requirements:***

- **Technology Infrastructure Assessment:** Detailed technical documentation of all systems
- **Security Architecture Review:** Comprehensive security controls evaluation
- **Operational Procedures:** Documented processes for all electronic banking functions
- **Risk Management Framework:** Identification and mitigation of technology risks
- **Customer Authentication:** Strong customer identification and authentication mechanisms

*3.1.3 **Compliance Implications for FinTech:***

- Must submit comprehensive technology documentation before launch
- Regular updates required for any system changes
- BDL reserves the right to audit all systems and processes
- Non-compliance can result in service suspension

3.1.3.1 Change Management and BDL Notifications

BDL Basic Circular 69/2000 not only mandates prior approval for launching new digital banking applications but also implies that significant changes or updates to approved systems may require re-notification or re-approval. FinTechs should establish a robust change management framework that includes:

1. **Impact Assessment:** Evaluate how proposed changes (e.g., new features, infrastructure upgrades, security control modifications) impact the initial BDL approval.
2. **Notification Triggers:** Define clear triggers for when BDL notification or re-approval is required (e.g., changes to core functionality, data handling, security architecture, or third-party integrations).
3. **Documentation:** Maintain detailed records of all changes, their assessments, and any communications or approvals received from BDL.
4. **Proactive Engagement:** Where there is ambiguity, proactively engage with BDL to clarify notification requirements to avoid non-compliance.

3.1.4 ISO 27001:2022 Alignment:*

- **A.5.1** Policies for information security
- **A.8.1** User endpoint devices
- **A.5.15** Access control
- **A.5.18** Authentication information

*References are to ISO/IEC 27001:2022 Annex A controls

3.2 BDL Basic Circular 144/2017 - Cybersecurity Measures

3.2.1 Comprehensive Security Framework

Issued on **November 28, 2017**, this circular mandates a comprehensive cybersecurity framework for banks and financial institutions. [12][13] It requires risk analysis, budget

allocation for cybersecurity, two-factor authentication, strong encryption in transit and at rest (In practice, the circular requires strong encryption in transit and at rest; many institutions interpret this as TLS 1.2/1.3 and robust at-rest encryption for sensitive data), continuous network monitoring, and penetration testing. [13] It also requires immediate reporting to BDL and the SIC for suspicious transactions and cyber incidents. [12]

Reference Link:

https://www.bdl.gov.lb/CB%20Com/Laws%20And%20Regulations/Basic%20Circulars/Decision_12725_EN%C2%A71410_3.pdf [13]

3.2.2 Detailed Requirements:

3.2.2.1 Authentication & Access Control:

- **Two-Factor Authentication (2FA):** Mandatory for all interactive user access to critical systems, all administrative/privileged accounts, and all remote access sessions. A risk-based approach may be documented for low-risk, internal-only systems.
- **Privileged Access Management:** Enhanced controls for administrative access
- **Session Management:** Automatic session timeouts and monitoring
- **Role-Based Access Control (RBAC):** Principle of least privilege enforcement

3.2.2.2 Encryption and Cryptography Standards:

- **Data at Rest:** AES-256 encryption minimum
- **Data in Transit:** Strong encryption (minimum TLS 1.2, with a preference for TLS 1.3) is mandatory for all internal and external communications transmitting sensitive data. This protects data as it moves across networks.
- **End-to-End (E2E) Application-Layer Encryption:** While not explicitly mandated across all systems, it should be implemented as a best practice where feasible for the most sensitive data (e.g., payment credentials, private messages) to provide the highest level of confidentiality.
- **Key Management:** Secure key generation, storage, and rotation

- **Digital Signatures:** Non-repudiation for critical transactions

3.2.2.3 Incident Response Requirements:

- **Prompt incident reporting to BDL for critical security incidents (generally interpreted as within 24 hours of confirmation).** Note that the Special Investigation Commission (SIC) must also be notified in cases involving suspicious financial transactions or money laundering.
- **Incident Classification:** Clear categorization of security incidents
- **Response Teams:** Dedicated cybersecurity incident response teams
- **Evidence Preservation:** Forensic capabilities for incident investigation

3.2.2.4 Security Testing:

- **Penetration Testing:** Annual third-party security assessments
- **Vulnerability Scanning:** Regular automated vulnerability assessments
- **Security Code Review:** Source code security analysis for custom applications
- **Red Team Exercises:** Simulated attack scenarios

3.2.3 ISO 27001:2022 Alignment:*

- A.5.15 Access control
- A.8.2 Privileged access rights
- A.8.3 Information access restriction
- A.10.1 Cryptographic controls
- A.16.1 Information security incident management

*References are to ISO/IEC 27001:2022 Annex A controls

3.3 BDL Basic Circular 141/2017 - Recovery Plans

3.3.1 Business Continuity & Disaster Recovery Framework

Issued on **September 18, 2017**, this circular requires Lebanese banks to prepare a detailed "Recovery Plan" to ensure they can restore financial stability during a crisis.

[14][15] The plan must be approved by the bank's Board of Directors, submitted to the Banking Control Commission (BCC) for assessment, and updated annually. [15]

Reference Link:

https://www.bdl.gov.lb/CB%20Com/Laws%20And%20Regulations/Basic%20Circulars/Decision_12670_EN%C2%A7219_3.pdf [15]

3.3.2 Core Requirements:

3.3.2.1 Recovery Plan Development:

- **Board Approval:** Board of directors must approve all recovery plans
- **BCC Submission:** Plans must be submitted to Banking Control Commission
- **Annual Review:** Mandatory annual review and updates
- **Scenario Planning:** Multiple disruption scenarios must be addressed

3.3.2.2 Recovery Objectives:

- **Recovery Time Objectives (RTO):** Maximum acceptable downtime for each service
- **Recovery Point Objectives (RPO):** Maximum acceptable data loss for each system
- **Minimum Service Levels:** Critical services that must be maintained during disruptions

3.3.2.3 Testing Requirements:

- **Regular Testing: At a frequency defined by risk and approved by the Board; quarterly is recommended best practice.**
- **Full-Scale Exercises:** Annual comprehensive disaster recovery exercises (recommended)
- **Documentation:** Detailed test results and lessons learned
- **Continuous Improvement:** Plan updates based on test outcomes

3.3.2.4 Alternative Site Requirements:

- **Geographic Separation:** DR sites must be geographically separated from primary sites

- **Lebanese Territory:** All alternative sites must be within Lebanese borders
- **Resource Availability:** Adequate resources to support critical operations
- **Communication Systems:** Alternative communication methods during disruptions

3.3.3 ISO 27001:2022 Alignment:*

- A.17.1 Information security continuity
- A.17.2 Redundancies

*References are to ISO/IEC 27001:2022 Annex A controls

3.4 BDL Basic Circular 128/2013 - Outsourcing Restrictions

3.4.1 Outsourcing Governance Framework

Issued on January 12, 2013, Basic Circular 128 (Decision 11323) requires banks and financial institutions to establish an autonomous, independent in-house Compliance Department (**comprising Legal Compliance and AML/CFT units**). [16] It also expressly prohibits outsourcing compliance monitoring, in whole or in part.

3.4.2 Core Provisions and Expectations

3.4.2.1 Non-Outsourceable (per Circular 128)

- **Compliance Monitoring:** May not be outsourced in whole or in part (Article 11). The Compliance Department must be in-house and independent (Articles 1–2).
- **Note on other control functions:** Circular 128 does not prohibit outsourcing Risk Management or Internal Audit; any expectations arise from other BDL instruments/supervisory practice. Institutions must retain independence, accountability, and oversight; external tools/co-sourcing may be used where permitted.
- **Decision-Making Authority:** Strategic and operational decisions must remain with the licensed institution. External providers may support operations and tooling, but the institution retains accountability.

3.4.2.2 Outsourcing Requirements (general good practice; align contracts accordingly)

- **Supervisory Access:** Agreements should enable supervisory access and information rights for BDL, the Banking Control Commission (BCC), and the SIC, as applicable, to review outsourced activities.
- **Contractual Protections:** Include clear SLAs, performance measures, confidentiality and data-protection clauses, liability/indemnity as appropriate, and remedies/penalties for non-performance.
- **Exit and Continuity:** Maintain documented exit/transition plans and business continuity/disaster recovery arrangements.
- **Notification/Approvals:** Where specific outsourcing notifications or approvals are required under other applicable BDL instructions, ensure timely compliance.

3.4.2.3 Vendor Management:

- **Due Diligence:** Thorough evaluation of service providers
- **Ongoing Monitoring:** Continuous monitoring of vendor performance
- **Risk Assessment:** Regular assessment of outsourcing risks
- **Contingency Planning:** Alternative arrangements in case of vendor failure

3.4.3 ISO 27001:2022 Alignment:*

- A.15.1 Supplier relationships
- A.15.2 Supplier service delivery management

*References are to ISO/IEC 27001:2022 Annex A controls

3.5 ⚖ Banking Secrecy Law of 1956

3.5.1 Foundation of Lebanese Banking Confidentiality (As Amended)

Originally enacted on September 3, 1956, this law established the principle of banking secrecy that was once a cornerstone of Lebanon's economy. [2][5] However, it has undergone significant amendments, notably with Law No. 306/2022 and **further clarifications* in early 2025**, in response to the economic crisis and to meet international

transparency standards required by bodies like the IMF. [2][3] While the law still protects client confidentiality, it is no longer absolute.

* Practitioners should verify current status and citations in the Official Gazette; language reflects market practice as of Aug 2025.

3.5.2 Key Provisions (Post-Amendment):

3.5.2.1 Confidentiality & Its Exceptions:

- **Strict Secrecy:** Bank employees are bound to secrecy regarding client names, assets, and related facts. Unauthorized disclosure is subject to criminal penalties. [6]
- **Expanded Exceptions:** The amendments have created crucial exceptions. Secrecy can now be lifted for a range of authorized entities, including:
    - The Judiciary and the Special Investigation Commission (SIC) for investigating financial crimes, corruption, and illicit enrichment. [2][3]
    - The Central Bank (BDL) and the Banking Control Commission (BCC) for supervisory and auditing purposes. [2][3]
    - The National Authority for Fighting Corruption. [4]
    - Tax authorities to verify compliance and combat evasion. [3]
    - Appointed independent auditors. [2][7]

3.5.2.2 Data Protection & Technology Implications:

- **Data Sovereignty:** The need for Lebanese authorities to have access for supervision and investigation reinforces the requirement for client data to remain within Lebanese jurisdiction.
- **Local Hosting:** Consequently, hosting systems with sensitive client financial data on international cloud platforms is practically unfeasible, as it would impede the legally mandated access and oversight of Lebanese regulatory bodies.
- **Access Controls:** Strict technical and procedural controls are required to manage and log access to client data, especially given the new legal exceptions.

3.5.3 *ISO 27001:2022* Alignment:*

- A.5.12 Classification of information
- A.5.34 Privacy and protection of personally identifiable information
- A.13.2 Information transfer

*References are to ISO/IEC 27001:2022 Annex A controls

4 Enhanced Compliance Requirements Matrix

4.1 Comprehensive Multi-Framework Mapping

Control Domain	BDL Requirement	ISO 27001:2022*	ISO 27017	Basel III	PCI DSS v4.0	Priority	Implementation Complexity	BDL Specificity
🔐 Data Sovereignty	Banking Secrecy Law	5.12, 5.34, 13.2	CLD.6.1.1, CLD.13.2.1	BCBS 239 Principle 11	Req 3.4, 12.8	CRITICAL	High	BDL Specific
🛡️ Access Controls	Circular 144/2017	5.15, 8.1, 8.2, 8.3	CLD.9.1.1, CLD.9.2.1	Operational Risk Mgmt	Req 7, 8	CRITICAL	Medium	BDL Enhanced
🔒 Encryption & Cryptography	Circular 144/2017	10.1	CLD.10.1.1, CLD.10.1.2	-	Req 3, 4, 8.3	CRITICAL	Medium	BDL Enhanced
🔄 Business Continuity	Circular 141/2017	17.1, 17.2	CLD.17.1.1, CLD.17.2.1	BCBS 239	Req 12.10	HIGH	High	BDL Specific
📋 Incident Management	Circular 144/2017	16.1	CLD.16.1.1	Operational Risk	Req 12.10	HIGH	Medium	BDL Enhanced
🤝 Supplier Management	Circular 128/2013	15.1, 15.2	CLD.15.1.1, CLD.15.2.1	Outsourcing Risk	Req 12.8	HIGH	High	BDL Specific
📊 Audit & Monitoring	Multiple Circulars	12.4, 12.7	CLD.12.4.1	BCBS 239	Req 10, 11	MEDIUM	Medium	BDL Enhanced

⚠️ Risk Management	Circular 69/2000	6.1, 6.2, 6.3	CLD.4.1.1	BCBS 239	Req 12.2	MEDIUM	High	Standard
🔍 Vulnerability Management	Circular 144/2017	12.6	CLD.12.6.1	-	Req 11	MEDIUM	Medium	Standard
👥 Personnel Security	Banking Secrecy Law	7.1, 7.2, 7.3	CLD.7.1.1	-	Req 12.7	MEDIUM	Low	BDL Enhanced

ISO control numbers in this table refer to ISO/IEC 27001:2022 Annex A.

4.2 Priority Classification System

4.2.1 CRITICAL (Risk Level 5)

- **Business Impact:** Service shutdown, regulatory penalties, criminal liability
- **Implementation Timeline:** Immediate (0-30 days)
- **Regulatory Consequence:** BDL license revocation

4.2.2 HIGH (Risk Level 4)

- **Business Impact:** Operational disruption, regulatory scrutiny
- **Implementation Timeline:** Short-term (30-90 days)
- **Regulatory Consequence:** Regulatory warnings, corrective action orders

4.2.3 MEDIUM (Risk Level 3)

- **Business Impact:** Compliance findings, operational inefficiency
- **Implementation Timeline:** Medium-term (90-180 days)
- **Regulatory Consequence:** Regulatory observations, improvement requirements

4.3 BDL Specificity Levels

4.3.1 ***BDL Specific***

Requirements unique to Lebanese banking regulation with no international equivalent

4.3.2 ***BDL Enhanced***

International standards enhanced with additional BDL-specific requirements

4.3.3 ***Standard***

Standard international requirements adopted by BDL

5 ISO 27001:2022 Control Mapping

5.1 Comprehensive Control Alignment

5.1.1 Clause 5: Leadership

ISO Control	BDL Requirement	Implementation Notes	BDL Gap
5.1 Policies for information security	Circular 69/2000	Board-approved security policies required	❌ None
5.12 Classification of information	Banking Secrecy Law	Must classify client data as highly confidential	❌ None
5.15 Access control policy	Circular 144/2017	2FA mandatory, enhanced access controls	❌ None
5.34 Privacy and PII protection	Banking Secrecy Law	Enhanced privacy protections, criminal penalties	❌ None

5.1.2 Clause 6: Planning

ISO Control	BDL Requirement	Implementation Notes	BDL Gap
6.1 Information security objectives	Circular 69/2000	Security objectives must align with BDL requirements	❌ None
6.2 Information security risk assessment	Multiple Circulars	Risk assessments must cover BDL-specific risks	❌ None
6.3 Information security risk treatment	Multiple Circulars	Risk treatment must ensure BDL compliance	❌ None

5.1.3 Clause 7: Support

ISO Control	BDL Requirement	Implementation Notes	BDL Gap
7.1 Resources	Not Specified	Companies must determine adequate resources	⚠️ Company Decision
7.2 Competence	Banking Secrecy Law	Staff must understand confidentiality requirements	❌ None
7.3 Awareness	Banking Secrecy Law	Enhanced awareness of secrecy obligations	❌ None

5.1.4 Clause 8: Operation

ISO Control	BDL Requirement	Implementation Notes	BDL Gap
8.1 Operational planning and control	Circular 69/2000	Operations must comply with BDL procedures	❌ None
8.2 Information security risk assessment	Multiple Circulars	Regular risk assessments required	❌ None
8.3 Information security risk treatment	Multiple Circulars	Risk treatment implementation	❌ None

5.1.5 Clause 10: Improvement

ISO Control	BDL Requirement	Implementation Notes	BDL Gap
10.1 Continual improvement	Circular 141/2017	Annual plan reviews and updates required	❌ None
10.2 Nonconformity and corrective action	Circular 144/2017	Incident response and corrective actions	❌ None

6 BDL Coverage Gaps & Company Decisions

6.1 ⚠ Areas Where BDL Provides Limited Guidance

6.1.1 🔧 Technical Implementation Details

6.1.1.1 Encryption Algorithms

While BDL mandates encryption, it does not specify algorithms. The following are industry-standard best practices that are highly recommended to meet regulatory expectations:

- **BDL Requirement:** “End-to-end encryption”
- **Company Decisions:**
  - Specific encryption algorithms (e.g. AES-256, RSA-4096)
  - Key management procedures
  - Encryption key rotation schedules
  - Hardware vs. software encryption choices

6.1.1.2 Authentication Methods

- **BDL Requirement:** “Two-factor authentication”
- **Company Decisions:**
  - Specific 2FA technologies (e.g. SMS, TOTP, hardware tokens)
  - Authentication strength requirements
  - Biometric authentication options
  - Single sign-on (SSO) implementations

6.1.2 🏗 Infrastructure Architecture

6.1.2.1 System Architecture Design

- **BDL Requirement:** “Technology infrastructure assessment”
- **Company Decisions:**
  - Microservices vs. monolithic architecture
  - Database design and optimization

- Load balancing and scalability approaches
- Container orchestration strategies

6.1.2.2 Network Security Design

- **BDL Requirement:** General security measures
- **Company Decisions:**
  - Network segmentation strategies
  - Firewall rule configurations
  - Intrusion detection/prevention systems
  - Network monitoring tools and procedures

6.1.3 Performance and Scalability

6.1.3.1 System Performance Requirements

- **BDL Gap:** No specific performance metrics
- **Company Decisions:**
  - Response time requirements
  - Throughput capacity planning
  - Scalability thresholds
  - Performance monitoring strategies

6.1.3.2 Capacity Planning

- **BDL Gap:** No capacity planning guidelines
- **Company Decisions:**
  - Growth projection methodologies
  - Resource allocation strategies
  - Infrastructure scaling triggers
  - Cost optimization approaches

6.1.4 Business Process Design

6.1.4.1 Customer Onboarding Processes

- **BDL Requirement:** Customer authentication
- **Company Decisions:**
  - KYC process design and workflows
  - Document verification procedures
  - Risk-based customer acceptance
  - Digital identity verification methods

6.1.4.2 Transaction Processing

- **BDL Requirement:** Secure transaction processing
- **Company Decisions:**
  - Transaction workflow design
  - Payment processing integration
  - Fraud detection algorithms
  - Transaction limits and controls

6.1.5 Monitoring and Analytics

6.1.5.1 Security Monitoring

- **BDL Requirement:** Incident detection and reporting
- **Company Decisions:**
  - SIEM tool selection and configuration
  - Security metrics and KPIs
  - Alerting thresholds and escalation
  - Threat intelligence integration

Inspection must be risk-based, documented, and aligned with secrecy and Law 81/2018

6.1.5.2 Business Analytics

- **BDL Gap:** No business intelligence requirements

- **Company Decisions:**
    - Data analytics frameworks
    - Reporting and dashboard design
    - Customer behavior analysis
    - Operational metrics tracking

6.2 🎯 Recommended Decision Framework

6.2.1 Risk-Based Decision Making

1. **Assess regulatory risk** for each technical decision
2. **Consider operational impact** of implementation choices
3. **Evaluate cost-benefit** of different approaches
4. **Document decision rationale** for regulatory review
5. **Plan for future regulatory changes**

6.2.2 Best Practice Alignment

- Follow international security standards where possible
- Seek BDL help for unclear requirements
- Implement defense-in-depth strategies
- Maintain comprehensive documentation
- Plan for regular reviews and updates

7 Data Sovereignty Requirements

7.1 LB Mandatory Local Hosting

7.1.1 Physical Infrastructure Requirements

✅ **Required:**

- All servers physically located within Lebanon
- Backup systems within Lebanese borders
- Network routing stays within Lebanon
- No data mirroring to external jurisdictions

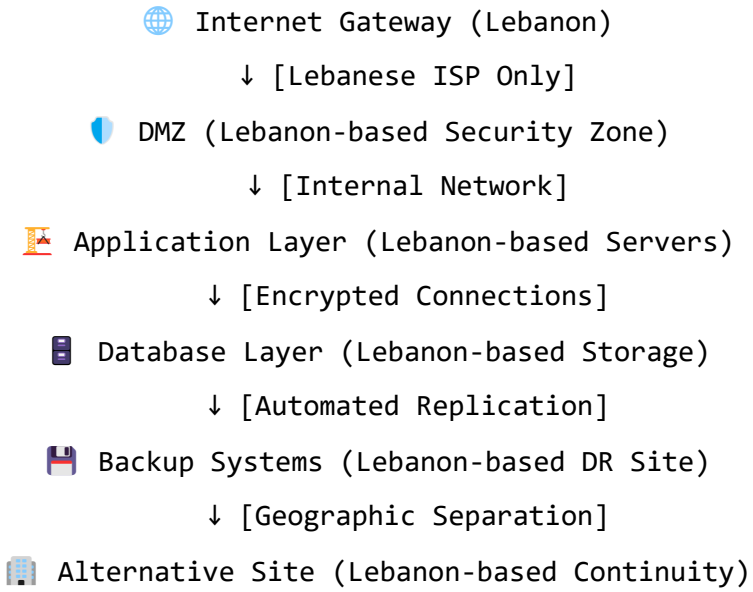
❌ **Prohibited:**

- International cloud providers (AWS, Azure, GCP) for production data and core regulated activities, due to the practical implications of data sovereignty and banking secrecy laws.
  https://www.mondaq.com/guides/results/10/1119/all/lebanon-fintech
- Backup replication to foreign data centers
- Data processing outside Lebanon
- **Uncontrolled remote access from outside Lebanon to production systems.** Any such access must be considered exceptional, justified by a formal risk assessment, and implemented with robust compensating controls (e.g., Privileged Access Management, session recording, multi-factor authentication, geo-fencing, and time-bound approvals), subject to BDL/BCC review.

7.1.2 Enhanced Data Classification Framework

Class	Data Examples	Core Requirements	Penalties	Hosting & Jurisdiction Mandate
Class 1: Banking Secrecy Protected (RED)	Customer personal information, KYC data, account details, transaction history, financial statements.	AES-256 encryption, strict access logging, Lebanese jurisdiction only.	Criminal liability under Banking Secrecy Law.	**Must be hosted within Lebanon on physically or logically segregated infrastructure. No cross-border replication or access without explicit legal basis and BDL approval.**
Class 2: Regulatory Protected (ORANGE)	System logs, audit trails, configuration data, regulatory reports, compliance documentation.	Access controls, audit trails, regulatory reporting capability.	Regulatory sanctions and fines.	**Must be hosted within Lebanon to ensure supervisory access for BDL/BCC. Can reside in an environment with strong logical separation.**
Class 3: Business Protected (YELLOW)	Internal system documentation, training materials, general operational data.	Standard security controls, backup procedures.	Business impact and reputational damage.	**Best practice is to host within Lebanon. If hosted externally, must be non-sensitive and justified by a risk assessment.**
Class 4: Public (GREEN)	Published documentation, marketing materials, public website content.	Basic security controls.	Minimal regulatory concern.	**No data residency restrictions. May be hosted globally (e.g., on a global CDN) for performance.**

7.2 Technical Implementation Architecture (Example Architecture)



8 Security & Risk Management

8.1 ISO 27001:2022/27017 Implementation for BDL Compliance

8.1.1 Enhanced Physical and Environmental Security

- **Data center security:** Biometric access, 24/7 CCTV monitoring, armed guards
- **Environmental controls:** Advanced fire suppression, precision climate control, redundant UPS
- **Equipment protection:** Secure destruction procedures, maintenance documentation
- **Lebanese jurisdiction:** All facilities within Lebanese borders

8.1.2 Advanced Access Control Management

- **Multi-factor authentication: Mandatory for privileged/admin, remote access, and critical systems; apply risk-based exceptions for low-risk internal systems with documented justification.**
- **Privileged access management:** Enhanced controls with session recording
- **Role-based access controls:** Principle of least privilege with regular reviews
- **Network segmentation:** Zero-trust architecture with micro-segmentation

8.1.3 Cryptographic Controls Enhancement

- **Data at rest:** AES-256 encryption with secure key management
- **Data in transit:** TLS 1.2/1.3 minimum for all communications
- **Key management:** Use of Hardware Security Modules (HSMs) is strongly recommended for managing cryptographic keys. **Recommended Target:** FIPS 140-2 Level 3 certification for the highest assurance, though Level 2 may be acceptable where justified by a risk assessment.
- **Digital signatures:** PKI infrastructure for non-repudiation

8.1.4 Comprehensive Incident Management (BDL Circular 144/2017)

- **24/7 Security Operations Center:** Continuous monitoring and threat detection

- **Automated incident detection:** SIEM integration with threat intelligence
- **Rapid response procedures:** Documented escalation and containment procedures
- **BDL notification:** Automated reporting within 24 hours for critical incidents
- **Forensic capabilities:** Evidence preservation and chain of custody procedures

8.2 ⚠ Enhanced Risk Assessment Framework (Basel III Alignment)

8.2.1 Expanded Risk Categories

- **Cybersecurity risks:** Advanced persistent threats, insider threats, supply chain attacks
- **Operational risks:** Process failures, human error, system outages
- **Regulatory risks:** Compliance failures, regulatory changes, penalty exposure
- **Reputational risks:** Public confidence, media coverage, customer trust
- **Financial risks:** Operational losses, penalty costs, business disruption

8.2.2 Risk Quantification Methodology (Example)

Risk Level	Probability	Financial Impact	Regulatory Impact	Response Timeline
Critical	>50%	>$1M	License suspension	Immediate (0-4 hours)
High	25-50%	$100K-$1M	Regulatory sanctions	Urgent (4-24 hours)
Medium	10-25%	$10K-$100K	Regulatory findings	Short-term (1-7 days)
Low	<10%	<$10K	Documentation issues	Medium-term (7-30 days)

9 Business Continuity & Disaster Recovery

9.1 Enhanced BDL Recovery Framework (Circular 141/2017)

9.1.1 Comprehensive Recovery Objectives (recommended – not BDL-mandated)

9.1.1.1 Tier 1: Critical Systems (Banking Core)

- **RTO:** 2 hours maximum downtime
- **RPO:** 5 minutes maximum data loss
- **Availability:** 99.9% annual uptime
- **Examples:** Core banking, payment processing, customer authentication

9.1.1.2 Tier 2: Important Systems (Customer Services)

- **RTO:** 8 hours maximum downtime
- **RPO:** 30 minutes maximum data loss
- **Availability:** 99.9% annual uptime
- **Examples:** Mobile banking, online portals, customer support systems

9.1.1.3 Tier 3: Supporting Systems (Operations)

- **RTO:** 24 hours maximum downtime
- **RPO:** 2 hours maximum data loss
- **Availability:** 99.5% annual uptime
- **Examples:** Reporting systems, analytics, administrative functions

9.1.2 Advanced Testing Requirements (recommended – not BDL-mandated)

9.1.2.1 Testing Schedule Matrix

Test Type	Frequency	Scope	Documentation Required
Component Testing	Monthly	Individual system components	Test results, issues identified
Partial Failover	Quarterly	Critical systems only	Full test report, lessons learned
Full DR Exercise	Semi-annually	Complete infrastructure	Board presentation, BCC submission
Crisis Simulation	Annually	Organization-wide response	Executive summary, improvement plan

9.2 Enhanced Shared Responsibility Model

9.2.1 Your Organization's Enhanced Responsibilities

✅ **Strategic and Operational:**

- Disaster declaration authority and decision-making
- Business impact assessment and prioritization
- Stakeholder communication and crisis management
- Regulatory compliance and BDL notification
- Customer communication and service restoration

✅ **Technical and Procedural:**

- Application-level testing and validation
- Data integrity verification post-recovery

- Business process continuity validation
- User acceptance testing and sign-off
- Performance benchmarking and optimization

9.2.2 Hosting Provider's Enhanced Responsibilities

✅ **Infrastructure and Technical:**

- Hardware availability and redundancy management
- Network connectivity and bandwidth provisioning
- Data replication and synchronization
- Storage systems and backup management
- Security infrastructure and monitoring

✅ **Support and Maintenance:**

- 24/7 technical support and escalation
- Infrastructure monitoring and alerting
- Preventive maintenance and updates
- Capacity planning and scaling
- Performance optimization and tuning

10 Proposed Implementation Roadmap *(Example)*

10.1 🚀 Enhanced 12-Month Implementation Timeline

10.1.1 ***Phase 1: Foundation & Assessment (Months 1-2)***

- ☐ **Week 1-2:** Complete comprehensive BDL regulation analysis
- ☐ **Week 3-4:** Conduct gap analysis against current infrastructure
- ☐ **Week 5-6:** Engage Lebanese legal counsel and compliance consultants
- ☐ **Week 7-8:** Develop preliminary compliance roadmap and budget

10.1.2 ***Phase 2: Planning & Design (Months 3-4)***

- ☐ **Week 9-12:** Design Lebanese-compliant technical architecture
- ☐ **Week 13-16:** Evaluate and select Lebanese hosting providers
- ☐ **Week 17-20:** Develop comprehensive security and compliance policies

10.1.3 ***Phase 3: Infrastructure Development (Months 5-7)***

- ☐ **Week 21-28:** Deploy Lebanese-based infrastructure and security controls
- ☐ **Week 29-32:** Implement monitoring, backup, and disaster recovery systems

10.1.4 ***Phase 4: Testing & Validation (Months 8-9)***

- ☐ **Week 33-36:** Conduct comprehensive security testing and vulnerability assessments
- ☐ **Week 37-40:** Perform disaster recovery testing and business continuity validation

10.1.5 ***Phase 5: Documentation & Submission (Months 10-11)***

- ☐ **Week 41-44:** Complete compliance documentation and evidence packages
- ☐ **Week 45-48:** Submit BDL applications and supporting documentation

10.1.6 ***Phase 6: Launch & Operation (Month 12)***

- ☐ **Week 49-52:** Go-live with regulatory approval, establish ongoing monitoring

10.2 💰 Budget Planning Framework *(Example)*

10.2.1 Infrastructure Costs (Annual)

- **Lebanese Data Center Hosting**
- **Security Infrastructure**
- **Disaster Recovery Site**
- **Network and Connectivity**

10.2.2 Compliance Costs (Annual)

- **Legal and Regulatory Consulting**
- **Security Assessments and Audits**
- **Compliance Software and Tools**
- **Training and Certification**

10.2.3 Operational Costs (Annual)

- **Compliance Staff**
- **Security Operations**
- **Monitoring and Maintenance**
- **Insurance and Bonding**

11 Hosting Provider Evaluation Framework

11.1 Critical Requirements Scorecard

11.1.1 Lebanese Jurisdiction Compliance (40 points)

- ☐ **Physical Infrastructure (10 points):** All servers within Lebanese borders
- ☐ **Data Sovereignty (15 points):** Guaranteed Lebanese data residency
- ☐ **Network Routing (10 points):** Domestic routing engineered and verified. If any unavoidable international transit occurs, strong encryption in-transit and documented ISP assurances are required to retain partial credit.
- ☐ **Legal Compliance (5 points):** Adherence to Lebanese regulations

11.1.2 Security and Certifications (30 points)

- ☐ **ISO 27001:2022 Certification (15 points):** Current and valid certification
- ☐ **ISO 27017 Cloud Security (10 points):** Cloud-specific security controls
- ☐ **Physical Security Controls (5 points):** Biometric access, 24/7 monitoring

11.1.3 Operational Excellence (20 points)

- ☐ **SLA Guarantees (8 points):** 99.9% uptime minimum with penalties
- ☐ **24/7 Lebanese Support (6 points):** Local technical support team
- ☐ **Disaster Recovery (6 points):** Lebanese-based DR site and procedures

11.1.4 Financial and Legal (10 points)

- ☐ **Financial Stability (5 points):** Audited financial statements
- ☐ **Insurance Coverage (3 points):** Professional liability and cyber insurance
- ☐ **Contract Terms (2 points):** Favorable terms and liability protection

11.2 Provider Evaluation Matrix

Evaluation Criteria	Weight	Provider A	Provider B	Provider C
Lebanese Jurisdiction	40%	___/40	___/40	___/40
Security & Certifications	30%	___/30	___/30	___/30
Operational Excellence	20%	___/20	___/20	___/20
Financial & Legal	10%	___/10	___/10	___/10
Total Score	100%	___/100	___/100	___/100

11.3 Due Diligence Questionnaire

11.3.1 Lebanese Compliance Verification

1. **Data Residency:** Can you provide written guarantee that our data will never leave Lebanese territory?
2. **Regulatory Access:** How do you facilitate BDL audit access as required by regulations?
3. **Legal Framework:** What Lebanese legal entities own and operate your infrastructure?
4. **Compliance Experience:** How many BDL-regulated entities do you currently serve?

11.3.2 Technical Capabilities Assessment

1. **Architecture:** Describe your network architecture and data flow within Lebanon
2. **Security Controls:** What technical controls prevent data export from Lebanon?

3. **Monitoring:** How do you monitor and detect potential data sovereignty violations?
4. **Incident Response:** What procedures do you have for security incidents affecting client data?

11.3.3 Business Continuity Evaluation

1. **DR Location:** Where is your disaster recovery site located within Lebanon?
2. **Recovery Testing:** How often do you test disaster recovery procedures?
3. **Communication:** How do you communicate during outages and incidents?
4. **Business Continuity:** What business continuity measures protect against provider failure?

12 Regulatory Reference Library

12.1 Primary BDL Regulations (Updated 2024)

12.1.1 ***Core Banking Circulars***

- **BDL Basic Circular 69/2000** - Electronic Banking Operations
  - *Original Issuance:* March 30, 2000. [8][9]
- **BDL Basic Circular 144/2017** - Cybersecurity Measures
  - *Original Issuance:* November 28, 2017. [12][13]
- **BDL Basic Circular 141/2017** - Recovery Plans
  - *Original Issuance:* September 18, 2017. [14][15]
- **BDL Basic Circular 128/2013** - Outsourcing Restrictions
  - *Original Issuance:* January 12, 2013. [16]

12.1.2 ***Specialized Circulars***

- **BDL Circular 146/2018** - GDPR Compliance Alignment: Requires institutions to take measures compliant with GDPR, including appointing a Data Protection Officer. [17][18]
- **BDL Circular 158/2021** - Exceptional measures for the gradual withdrawal of deposits in foreign currencies: Sets a framework allowing eligible depositors to withdraw limited amounts (e.g., ~$800/month) from older foreign currency accounts. [19][20]
- **BDL Circular 162/2022** - Payment of Public Sector Employees Salaries: Mandates that banks must allow public sector employees to fully withdraw their monthly salaries without imposing any caps or restrictions. [21][22]
- **BDL Circular 171/2022** - Exceptional restrictions relating to some banking operations: Part of a series of crisis-management circulars imposing temporary restrictions on certain banking activities. [23]

12.2 Supporting Lebanese Legislation

12.2.1 Financial Services Laws

- **Code of Money and Credit (1963)** - Foundation of Lebanese banking law
- **Banking Secrecy Law of 1956** - Client confidentiality and data protection **(as amended by Law No. 306/2022 and subsequent clarifications in 2025 to broaden supervisory access)**
- **Electronic Transactions and Personal Data Law (Law 81/2018)** - Digital privacy framework
- **Anti-Money Laundering Law (Law 44/2015)** - AML/CTF requirements

12.2.2 Technology and Data Protection

- **Cybercrime Law (Law 140/2018)** - Computer crimes and digital evidence
- **Electronic Signature Law (Law 586/2004)** - Digital signature validation
- **Consumer Protection Law** - Customer rights and data handling

12.3 International Standards Alignment

12.3.1 ISO Security Standards

- **ISO 27001:2022** - Information Security Management Systems
- **ISO 27017:2015** - Cloud Security Controls and Guidelines
- **ISO 27018:2019** - Cloud Privacy Controls
- **ISO 22301:2019** - Business Continuity Management

12.3.2 Financial Industry Standards

- **Basel III Framework** - International banking regulations
- **PCI DSS v4.0** - Payment Card Industry Security Standards
- **SWIFT Customer Security Programme (CSP)** - Financial messaging security
- **NIST Cybersecurity Framework** - Risk-based cybersecurity guidance

12.3.3 Regional and International Compliance

- **EU GDPR** - European data protection regulation (where applicable)

- **FATCA** - US tax compliance requirements
- **CRS** - Common Reporting Standard for tax information exchange

12.4 📞 Official BDL Contact Directory (should be verified)

12.4.1 ***Primary Regulatory Contacts***

Banking Control Commission (BCC): For official inquiries, please refer to the contact page on the official BDL or BCC website. Publicly listed numbers should be verified before use.

13 Quick Reference Compliance Checklist

13.1 CRITICAL - Immediate Action Required

- ☐ ✅ **Data Sovereignty:** All data hosted within Lebanese borders
  - *Evidence Example: Lebanese data center residency letter; network routing verification.*
- ☐ ✅ **BDL Approval:** Submitted application for electronic banking operations
  - *Evidence Example: BDL submission ID; approval letter.*
- ☐ ✅ **Two-Factor Authentication:** Implemented for privileged/admin, remote access, and critical systems; risk-based approach documented for low-risk internal systems.
  - *Evidence Example: 2FA implementation report; access control matrix*
- ☐ ✅ **Incident Reporting:** 24-hour BDL notification procedures established
  - *Evidence Example: Incident response plan; sample incident report.*
- ☐ ✅ **Banking Secrecy Compliance:** Client data confidentiality measures active
  - *Evidence Example: Data classification policy; access logging reports.*

13.2 HIGH - Short-Term Implementation (30-90 days)

- ☐ 🟡 **Business Continuity Plan:** Board-approved and submitted to BCC
  - *Evidence Example: Board resolution; BCC submission confirmation.*
- ☐ 🟡 **Security Assessments:** Annual penetration testing scheduled
  - *Evidence Example: Penetration test report; vulnerability scan results.*
- ☐ 🟡 **Encryption Standards:** Strong encryption in transit (TLS 1.2/1.3) and encryption at rest (e.g., AES-256). Where feasible, apply application-layer encryption for the most sensitive data.
  - *Evidence Example: Encryption policy; cryptographic key management plan; HSM attestation.*

- ☐ 🟡 **Access Controls:** Role-based access with privileged user monitoring
  - *Evidence Example: Role-based access matrix; PAM session recording samples.*
- ☐ 🟡 **Audit Capabilities:** BDL supervisory access to all systems
  - *Evidence Example: Audit log review procedures; BDL access protocols.*

13.3 MEDIUM - Medium-Term Goals (90-180 days)

- ☐ 🟢 **ISO 27001:2022:** Certification process initiated
  - *Evidence Example: Certification roadmap; audit schedule.*
- ☐ 🟢 **Vendor Management:** Lebanese hosting provider contracts finalized
  - *Evidence Example: Signed contracts; due diligence reports.*
- ☐ 🟢 **Risk Framework:** Comprehensive risk assessment completed
  - *Evidence Example: Risk assessment report; risk register.*
- ☐ 🟢 **Staff Training:** Banking secrecy and compliance training delivered
  - *Evidence Example: Training records; attendance sheets.*
- ☐ 🟢 **Documentation:** Complete compliance evidence package prepared
  - *Evidence Example: Document control register; evidence repository link.*

14 Implementation Success Factors

14.1 Critical Success Enablers

1. **Executive Leadership:** Strong C-level commitment to compliance investment
2. **Lebanese Partnerships:** Relationships with compliant local service providers
3. **Regulatory Engagement:** Proactive communication with BDL compliance teams
4. **Conservative Approach:** Exceeding minimum requirements to ensure compliance
5. **Continuous Monitoring:** Ongoing assessment of regulatory changes and updates

14.2 Competitive Advantages of Compliance

1. **Market Access:** Full access to Lebanese banking and financial services market
2. **Customer Trust:** Enhanced credibility with Lebanese financial institutions
3. **Regulatory Relationships:** Positive standing with BDL and regulatory authorities
4. **Risk Mitigation:** Protection against significant regulatory penalties and sanctions
5. **Operational Resilience:** Robust infrastructure and business continuity capabilities

15 Future Regulatory Trends *(Our expectations)*

15.1 Expected BDL Developments (2025-2027)

- **Digital Currency Regulation:** Comprehensive framework for CBDCs and stablecoins
- **AI Governance and Machine Learning Guidelines:** Risk management for automated decision-making
- **Open Banking Standards:** API security and data sharing requirements
- **Enhanced Cybersecurity:** Zero-trust architecture and advanced threat protection
- **Cloud Computing Framework:** Potential relaxation of current restrictions with enhanced controls

15.2 International Alignment Initiatives

- **Basel IV Implementation:** Enhanced operational risk and technology risk management
- **FATF Recommendations:** Strengthened AML/CTF technology requirements
- **EU Digital Finance Package:** Potential alignment with European digital asset regulations
- **Regional Cooperation:** Enhanced coordination with regional banking authorities

16 Conclusion

Lebanese FinTech companies operating in today's regulatory environment must navigate complex requirements that prioritize data sovereignty, security, and traditional banking principles. Success in this environment requires:

16.1 Strategic Imperatives

1. **Lebanese-First Infrastructure:** All technology infrastructure within Lebanese borders
2. **Conservative Compliance Approach:** Exceed minimum requirements to ensure regulatory confidence
3. **Strong Local Partnerships:** Collaborate with experienced Lebanese hosting and service providers
4. **Comprehensive Documentation:** Maintain thorough evidence of compliance across all requirements
5. **Continuous Monitoring:** Establish ongoing compliance monitoring and regulatory relationship management

16.2 Competitive Differentiation

Organizations that successfully implement comprehensive BDL compliance frameworks position themselves as:

- **Trusted Partners** for Lebanese financial institutions
- **Preferred Vendors** for government and enterprise clients
- **Market Leaders** in regulatory compliance and risk management
- **Growth Platforms** for regional expansion and partnership opportunities

16.3 Long-Term Value Creation

Investment in robust BDL compliance creates lasting competitive advantages through:

- **Regulatory Capital:** Strong relationships and positive standing with authorities
- **Operational Excellence:** Resilient infrastructure and business continuity capabilities
- **Market Position:** Differentiated offering in compliance-critical market segments
- **Risk Management:** Comprehensive protection against regulatory and operational risks

This guide provides the comprehensive foundation for building a successful, compliant FinTech operation in Lebanon. The regulatory landscape will continue to evolve, and organizations must remain vigilant and adaptive to maintain their competitive position.

For specific implementation guidance, organizations should engage qualified Lebanese legal counsel, compliance professionals, and certified hosting providers familiar with BDL requirements.

17 Glossary of Key Terms and Acronyms

- **BDL:** Banque du Liban, the central bank of Lebanon.
- **BCC:** Banking Control Commission, the primary supervisory body for banks and financial institutions in Lebanon.
- **FinTech:** Financial Technology, referring to technology-enabled innovation in financial services.
- **HSM:** Hardware Security Module, a physical computing device that safeguards and manages digital keys for strong authentication.
- **KYC:** Know Your Customer, the mandatory process of identifying and verifying the identity of a client.
- **PAM:** Privileged Access Management, a cybersecurity strategy and toolset for controlling and monitoring access for administrative and other high-privilege accounts.
- **PCI DSS:** Payment Card Industry Data Security Standard, a global security standard for all entities that store, process, or transmit cardholder data.
- **RPO (Recovery Point Objective):** The maximum acceptable amount of data loss following an incident, measured in time (e.g., 5 minutes of data).
- **RTO (Recovery Time Objective):** The maximum acceptable length of time that a system can be down after a disruption.
- **SIC:** Special Investigation Commission, Lebanon's Financial Intelligence Unit (FIU) responsible for investigating suspicious transactions related to money laundering and terrorism financing.
- **SIEM:** Security Information and Event Management, a solution that provides real-time analysis of security alerts generated by applications and network hardware.

18 Appendix A: Pre-Submission Pack to BDL (Artifact Index)

This appendix provides a checklist of key documents and artifacts typically required for submission to the Banque du Liban (BDL) or the Banking Control Commission (BCC) for various regulatory approvals and ongoing compliance. This list is illustrative and should be adapted based on the specific submission requirements.

- **Corporate and Licensing Documents:**

☐ Company Registration Certificate

☐ BDL Operating License (if applicable)

☐ Board of Directors Resolution for the proposed service/system

☐ Organizational Chart (highlighting compliance and IT functions)

☐ Audited Financial Statements

- **Technology & Security Documentation:**

☐ Detailed System Architecture Diagram (highlighting Lebanese-only infrastructure)

☐ Technology Infrastructure Assessment Report (per BDL Circular 69/2000)

☐ Security Architecture Review Report

☐ Data Flow Diagrams (showing data residency within Lebanon)

☐ Data Classification Policy and Register

☐ Access Control Matrix

☐ Encryption Policy and Key Management Plan

☐ Cybersecurity Framework Document (per BDL Circular 144/2017)

☐ Penetration Testing Reports (annual)

☐ Vulnerability Assessment Reports (regular)

☐ Security Incident Response Plan (per BDL Circular 144/2017)

☐ Forensic Capabilities Documentation

- **Business Continuity & Recovery Documentation:**

☐ Board-Approved Business Continuity Plan (BCP) (per BDL Circular 141/2017)

☐ Disaster Recovery Plan (DRP)

☐ Recovery Time Objective (RTO) and Recovery Point Objective (RPO) Declarations

☐ BCP/DRP Testing Reports (including full-scale exercises)

☐ Alternative Site Readiness Documentation

- **Outsourcing & Vendor Management:**

☐ Outsourcing Policy

☐ Signed Contracts with Lebanese Hosting Providers/Third Parties (including BDL's right-to-audit clauses)

☐ Third-Party Due Diligence Reports

☐ Exit Strategies for Outsourced Services

- **Compliance & Legal:**

☐ Compliance Monitoring Plan

☐ Staff Training Records (especially for Banking Secrecy Law)

☐ Legal Opinion on Data Sovereignty and Banking Secrecy Law Compliance

☐ AML/CFT Policies and Procedures

- **Operational Procedures:**

☐ Customer Onboarding Procedures (including KYC)

- ☐ Transaction Processing Workflows
- ☐ Change Management Policy and Procedures
- ☐ Operational Procedures for Electronic Banking Functions

Disclaimer: This guide is intended solely as a comprehensive public reference and informational resource. It provides general guidance based on publicly available BDL regulations and international best practices as of August 2025.

Capital Outsourcing SAL, its employees (including the author), and affiliates are not providing legal, financial, or specific compliance advice through this document. The content herein does not constitute a substitute for professional advice tailored to an individual FinTech entity's specific circumstances, licensing status, or business model.

Regulatory requirements are subject to change, and their interpretation and application can vary. Therefore, specific legal and compliance advice from qualified professionals should always be sought for all implementation decisions.

Capital Outsourcing SAL expressly disclaims any and all liability for any direct, indirect, or consequential loss or damage whatsoever arising from the use of, or reliance on, this guide or any information contained within it. Users of this guide assume full responsibility for their decisions and actions based on its content.

Author: Abed Al Rahman Naboulsi - Information Security Officer, Capital Outsourcing SAL
Version Control: v1.0 - Enhanced comprehensive edition

Learn more:

1. Lebanon FinTech Comparative Guide - All Chapters - Mondaq
2. Banking secrecy amendments ditch real estate and non-bank sectors, a reform to wipe deposits? - Nowlebanon
3. Lebanon's Amended Banking Secrecy Law: Causes and Consequences - Fanack
4. Lebanon Reforms Banking Secrecy Law Amid Deepening Economic Crisis
5. Lifting Banking Secrecy: A Major Shift in Lebanon's Financial System
6. Facts about the Lebanese Banking Sector - Main Banking & Financial Regulations
7. Stronger lift by Parliament of banking secrecy provisions. Allows ten-year retrospective
8. Document library » BDL Basic Circular - 69: Electronic Banking and Financial Operations
9. 1 BANQUE DU LIBAN Basic Circular 69 addressed to Banks, And also to Financial Institutions and Institutions Engaged in Electro
10. BANQUE DU LIBAN Basic Circular No 69 addressed to Banks, And also to Financial Institutions and Institutions Engaged in Electronic
11. BDL Basic Circular No. 69 - Special Investigation Commission
12. BDL Issued Circular No.144 on Nov.28th 2017 to Protect Banks Against Financial Cybercrime - BLOMINVEST
13. 1 Basic Circular No 144 Addressed to Banks and Financial Institutions Attached is a copy of Basic Decision No 12725 of 28 Novemb - Banque Du Liban
14. BDL Basic Circular 141: Recovery Plan - Document Library - Economena Analytics
15. 1 Basic Circular No 141 Addressed to Banks Attached is a copy of Basic Decision No 12670 of September 18, 2017 relating to the R - Banque Du Liban
16. BANQUE DU LIBAN Basic Circular No. 128 Addressed to Banks and Financial Institutions
17. What you should know about GDPR, and why it matters to you - Saradar Bank
18. Document library » BDL Basic Circular - 146: General Data Protection Regulation (GDPR)
19. BDL Circular 158: Gradual Withdrawal of Foreign Currency Deposits | Bank of Beirut
20. BDL Circular 158 on gradual withdrawal of deposits (UPDATED)
21. BDL ISSUES BASIC CIRCULAR 162 PERTAINING TO THE REIMBURSEMENT OF PUBLIC SECTOR SALARIES - Credit Libanais - Economic Research
22. Banque du Liban issues Circular 162 that demands banks to place no restrictions on payment of public sector employees' salaries and allowances | Civil Society Knowledge Centre
23. basic circulars - Banque Du Liban