OPERATIONAL RISK MANAGEMENT MODULE

MODULE	OM Operational Risk Management
Table of Contents	

OM-A.3 Module History

OM-A.3.1 This Module was first issued in July 2004 as part Volume one of the CBB Rulebook (Volume one). All directives in this Module have been effective since this date. Any material changes that have subsequently been made to this Module are annotated with the calendar quarter date in which the change was made; Chapter UG-3 provides further details on Rulebook maintenance and version control.

OM-A.3.2 When the CBB replaced the BMA in September 2006, the provisions of this Module remained in force. Volume 1 was updated in October 2007 to reflect the switch to the CBB; however, new calendar quarter dates were only issued where the update necessitated changes to actual requirements.

OM-A.3.3 The most recent changes made to this Module are detailed in the table below:

Summary of Changes

Module Ref.	Change Date	Description of Changes
OM-5.1	01/04/05	Physical security measures.
OM-4.2	01/10/05	Succession planning for locally incorporated banks.
OM-5.1	01/10/05	Clarification of security manager role for smaller banks.
OM-B & OM-1.2	01/04/06	Minor amendments concerning roles of Board and management.
OM-5.1.15-24	01/04/06	New security requirements for ATMs and reporting of security related complaints.
OM-A.2.1-6	01/10/07	Purpose (expanded)
OM-A.2.1-6	01/10/07	Key Requirements (deleted)
OM-2.1-2.2 & 2.4	01/10/07	Relocation of Succession Planning Requirements from OM-4
OM-5.1-OM-5.9	01/10/07	Business Continuity Planning (expanded)
OM-7	01/10/07	Books and Records Chapter transferred from Module GR
OM-8	01/04/08	Basel II Qualitative Operational Risk Requirements
OM	01/2011	Various minor amendments to ensure consistency in CBB Rulebook.
OM-A.1.3 and OM-A.1.4	01/2011	Clarified legal basis.
OM-7.1.4	04/2011	This Paragraph was deleted as Ministerial Order 23 does not apply to CBB licensees.
OM-7.3.4	04/2011	Clarified retention period of records for promotional schemes.
OM	07/2011	Various minor amendments to clarify Rules and have consistent language.
OM-2.4	07/2011	Amended CBB reporting requirements regarding succession planning.
OM-3.1.7	07/2011	Paragraph deleted as no longer applicable since standard conditions and licensing criteria document has now been incorporated as part of Volume 1.
OM-6.2	10/2011	Added new Section on internet security.
OM-7.1.7	10/2011	Corrected typo.
OM-A.1.3	01/2012	Updated legal basis.
OM-2.1.4	01/2012	Corrected cross reference.
OM-3.2.2	04/2012	Deleted last sentence of Paragraph as it repeats the requirement under Paragraph OM-3.3.1
OM-6.2.2	04/2012	Clarified penetration testing interval for internet security.
OM-1.1.4	10/2012	Amended to reflect updated version of Basel Committee document.
OM-3.2.6, OM-5.2.1, OM-5.4.8, OM-8	10/2012	Amended to reflect the Basel June 2011 paper on Principles for the Sound Management of Operational Risk.

OM-A.3 Module History (continued)

OM-A.3.3 (continued)

Summary of Changes

Module Ref.	Change Date	Description of Changes
OM-6.2	07/2013	Amended reporting requirements related to internet security measures.
OM-6.2.1	10/2013	Amended Rule to apply to all banks.
OM-6.2.1	04/2015	Clarified that penetration testing services must be undertaken by external independent parties that are not employees of the bank nor associated with it.

Evolution of the Module

OM-A.3.4 [Deleted in October 2007 updates]

OM-3.8 Intra-group Outsourcing

OM-3.8.1 **As with outsourcing to non-group companies, the Board and management of licensees are held ultimately responsible by the CBB for the adequacy of systems and controls in activities outsourced to group companies.**

OM-3.8.2 However, the degree of formality required – in terms of contractual agreements and control mechanisms – for outsourcing within a licensee's group is likely to be less, because of common management and enhanced knowledge of other group companies.

OM-3.8.3 **A licensee must formally notify the CBB at least 6 weeks before committing to a material intra-group outsourcing. The request must be made in writing to the licensee's normal supervisory contact, and must set out a summary of the proposed outsourcing, its rationale, and an analysis of its associated risks and proposed mitigating controls. The CBB will respond to the notification in the same manner and timescale as set in Section OM-3.3 above.**

OM-3.8.4 The CBB expects, as a minimum, an agreed statement of the standard of service to be provided by the group provider, including a clear statement of responsibilities allocated between the group provider and licensee.

OM-3.8.5 The CBB also expects a licensee's management to have addressed the issues of customer confidentiality, access to information and business continuity covered above (Section OM-3.5).

OM-3.8.6 For further rules on intragroup outsourcing of functions containing customer information, see OM-3.9.7.

OM-3.9 Outsourcing of Functions Containing Customer Information

Third Party Outsourcing of Functions Containing Customer Information

OM-3.9.1 **The requirements in this Section are applicable to the outsourcing of functions/services involving customer information, including but not limited to card processing and electronic/internet banking services.**

OM-3.9.2 **Because of the critical importance of functions containing customer information, all proposals to outsource such functions/operations are to be considered material.**

OM-3.9.3 For further clarification, services such as web design, web hosting and card printing/mailing, IT technological support, Admin support and Internal Audit are not subject to the requirements of this section. For rules on internal audit outsourcing, see OM-3.7.

OM-3.9.4 **Licensees are allowed to outsource functions containing customer information, if required, only to service providers licensed by the CBB and located in Bahrain.**

OM-3.9.5 **Licensees must ensure that service providers do not sub-outsource the function/service to third party service providers.**

OM-3.9.6 The CBB reserves the right to require a licensee to terminate or make alternative outsourcing arrangements if the confidentiality of its customer information or the ability of the CBB to carry out its supervisory functions cannot be assured.

OM-3.9 Outsourcing of Functions Containing Customer Information (Continued)

Intra-group Outsourcing of Functions Containing Customer Information

OM-3.9.7 In addition to the requirements under Section OM-3.8, the CBB may allow intra-group outsourcing of functions containing customer information, subject to the following conditions:

(a) The outsourcing provider is the head office of the licensee which is regulated by the financial regulator of the home jurisdiction;

(b) All of the group's subsidiaries providing the outsourcing activity are regulated by the financial regulator of the jurisdiction where they are located; and

(c) Where the outsourcing provider is one of the group's unregulated subsidiaries the following conditions must be met:

i. The outsourcing service providers must be regularly audited with regard to the adequacy and effectiveness of control by the Group Internal Audit team and the audit findings must be reported to the CBB immediately;

ii. The service level agreement must clearly state that the CBB has the right to conduct onsite examinations of the outsourcing provider (expenses to be borne by the licensee) with the objective of evaluating the adequacy and effectiveness of internal controls, in accordance with the CBB's relevant rules.;

iii. Any report by any other regulatory authority on the review/audit of the subsidiary must be submitted immediately by the respective licensee to the CBB; and

iv. Where customer information is shared with the licensee's subsidiaries, prior written customer consent must be obtained.

OM-3.10 Transitional Arrangements

OM-3.10.1 This Section issued in XX 201X, is effective on 1st January 201X. All conventional bank licensees to which Module OM applies must be in full compliance with this Chapter by the financial year end 201X.

OM-3.10.2 In cases where the required type of service is not available in Bahrain, after XX 201X, outsourcing to service providers outside Bahrain will be allowed by the CBB, for a maximum period of 2 years, subject to the following conditions:

(a) A written request must be submitted to the CBB, at least 30 days before the end of the transition period, stated in OM-3.10.1, detailing the circumstances under which the extension of outsourcing activities is being requested;
(b) Outsourcing outside Bahrain must be conducted in a manner so as not to hinder efforts to supervise or reconstruct the Bahrain activities of the licensee (i.e. from its books, accounts and documents) in a timely manner;
(c) Licensees must, enter into arrangements only with parties operating in jurisdictions that uphold confidentiality clauses and agreements;
(d) Licensees must not outsource to jurisdictions where prompt access to information by the CBB or its appointed representatives may be impeded by legal or administrative restrictions;
(e) Licensees must provide written confirmation to the CBB, that the CBB would be granted the right to access all the licensee's information, reports and findings at the service provider; and
(f) Licensees must immediately notify the CBB if any overseas authority were to seek access to its customer information or if a situation were to arise where the rights of access of the licensee and the CBB have been restricted or denied.

OM-3.10 Transitional Arrangements (Continued)

OM-3.10.3 The CBB may require additional measures to be taken by a licensee, depending on the potential impact of the outsourcing on the licensee and the financial system, or as circumstances warrant, the CBB may also directly communicate, where applicable, with the home or host regulator of the service provider, on their ability and willingness to cooperate with the CBB in supervising the outsourcing risks to the licensee.

OM-3.10.4 Licensees must notify the CBB of the steps taken to find alternative solutions for the outsourced service/activity required from outside Bahrain, at least 3 months prior to the completion of the 2 years period, stated in OM-3.10.2.

OM-6.1 Physical Security Measures (continued)

Cash Safety

OM-6.1.12 Cash, precious metals, and bearer instruments must be kept in fireproof cabinets/safes. These cabinets/safes must be located in strong rooms.

OM-6.1.13 Strong rooms must be made of reinforced solid concrete, or reinforced block work. Doors to strong rooms must be made of steel and preferably have a steel shutter fitted. Dual locking devices must be installed on strong room doors. Strong room doors must be located out of the sight of customers.

OM-6.1.14 Strong rooms must not contain any other openings except the entry door and where necessary, an air conditioning outlet. The air conditioning outlet must be protected with a steel grill.

OM-6.1.15 This paragraph was deleted in April 2015.
~~ATMs should not normally be replenished during customer opening hours. Replenishment of off-site ATMs must be performed by specialised service providers, comprising a crew of at least two persons. ATM replenishment staff must carry a mobile phone or communication device in case of emergency.~~

OM-6.1.16 This paragraph was deleted in April 2015.
~~All cash movements between branches, to and from the CBB and to off-site ATMs must be performed by specialised service providers.~~

OM-6.1.17 This paragraph was deleted in April 2015.
~~All ATMs must be properly maintained and covered by service or maintenance agreements. All ATMs must be inspected daily by bank staff to check that they are functioning properly and have not been tampered with.~~

OM-6.1.18 This paragraph was deleted in April 2015.
~~All banks must maintain a list of all maintenance, replenishment and inspection visits by staff or other authorised parties.~~

OM-6.1.19 This paragraph was deleted in April 2015.
~~All ATMs must be fitted with fraud detection and inhibiting devices (mandatory after year end 2006).~~

OM-6.1 Physical Security Measures (continued)

CCTV Network Systems

OM-6.1.20 All head offices and branches must at all times have an operating CCTV network and alarm system which are ~~which is~~ connected to a central monitoring unit located in the head office, along with a Video Monitoring System (VMS)~~and to the MOI Central Monitoring Unit~~.

OM-6.1.21 ~~The location and type of CCTV cameras is left to the discretion of banks.~~ At a minimum, CCTV cameras must cover the following areas:

(a) Main entrance;
(b) Other external doors;
(c) Any other access points (e.g. ground floor windows);
(d) The banking hall;
(e) Tellers' area;
(f) Strongroom entrance; and
(g) ATMs (by way of internal or external cameras) – Refer to OM-6.3 for specific CCTV requirements related to ATMs.

OM-6.1.22 Notices of CCTV cameras in operation must be displayed in an area or areas which are easily accessible to the public. CCTV records must be retained in a secure area for a minimum 90-day period. The transmission rate (in terms of the number of frames per second) must be sufficient to ensure effective monitoring of the relevant areas. All transmission must be in real time, and under no circumstances is delayed transmission of pictures to the Central Monitoring Unit acceptable. The CCTV system must be operational 24 hours per day every day of the year, including when the bank is closed for business.

OM-6.1 Physical Security Measures (continued)

Training and Other Measures

OM-6.1.23 **Banks must have a designated security manager. This person will be responsible for all aspects of physical security, including ensuring all bank staff are given annual, comprehensive security training. Banks must have a Board-approved security manual supplemeted by appropriate documented procedures for staff, especially those dealing directly with customers. For banks with three or more branches, this position must be a formally identified position. For banks with one or two branches, the responsibilities of this position may be added to the duties of a member of management.**

OM-6.1.24 **The security manager must maintain records concerning security-related complaints by customers and take corrective action or make recommendations for action on a timely basis. Actions and recommendations must be documented.**

OM-6.1.25 **Banks must consider safety and security issues when selecting premises for new branches. Key security issues include prominence of location (e.g is the branch on a main street or a back street?), accessibility for emergency services, an assessment of surrounding premises (in terms of their safety or vulnerability), and the number of points of entry and/or egress to/from the branch. All banks are required to hold an Insurance Blanket Bond (the cover of which includes reimbursement for the theft of cash).**

OM-6.1.26 For further rules on ATM Physical Security Measures, see OM-6.4.

OM-6.2 Internet Security

OM-6.2.1 All banks providing internet banking services must regularly test their systems against security breaches and verify the robustness of the security controls in place. These tests must be conducted by security professionals, such as ethical hackers, that provide penetration testing services and a vulnerability assessment of the system. The tests must be undertaken by external independent parties that are not employees of the bank nor associated with it.

OM-6.2.2 The penetration testing referred to in Paragraph OM-6.2.1, must be conducted each year in June and December.

OM-6.2.3 The vulnerability assessment report, along with the steps taken to mitigate the risks must be retained by the bank for at least a 5-year period from the date of testing and must be provided to the CBB within two months following the end of the month in which the testing took place, e.g. for the June test, the report must be submitted at the latest by 31st August and for the December test, by 28th February (see Section BR-4A.2).

OM-6.3 ATM Security Measures: Hardware/Software

Implementation

OM-6.3.1 The requirements in this Section must be complied with in full within 6 months from its issuance. Failure to comply with these requirements will trigger a supervisory response, which may include formal enforcement measures, as set out in Module EN (Enforcement).

Geolocation Limitations

OM-6.3.2 All retail banks issuing debit, prepaid and/or credit cards must ensure that all Bahrain issued cards enable each customer to maintain a list of 'approved' countries for card ATM/Point of Sale (POS) transactions. Customers must be allowed to determine those countries in which their card must not be accepted as well as countries or merchant categories in which a card transaction would require a further level of authorisation, (for example, 2 way sms).

Integration of Hardware Components

OM-6.3.3 Banks must ensure that the Electronic PIN Pad (EPP) on the ATM complies with the security approval criteria required by, and amended from time to time, in the Payment Card Industry Security Standards Council (PCI SSC) (web site (https://www.pcisecuritystandards.org)).

OM-6.3.4 If the Automated Teller Machines (ATM) environment permits access to internal areas where account data is processed and/or stored (e.g., for service or maintenance), these areas must be effectively protected from access by unauthorised persons to mitigate the risk associated with attaching/inserting malicious additional components, especially those which may be designed to capture sensitive data. Banks must encrypt account data or secure access to such data by effective physical barriers such as strong walls, doors, and mechanical locks.

OM-6.3.5 All entry to sensitive areas must be recorded, including the name of the persons accessing the area; the date; and the time of access to and exit from the area. CCTV cameras must be installed, and used to record all activities within the ATM environment.

OM-6.3 ATM Security Measures : Hardware/Software (Continued)

OM-6.3.6 As a precursor to installing the ATM, it is essential to list the security options which have been incorporated by the manufacturer and where applicable any and all customized functions which have been incorporated by or at the request of the bank. This data must be updated without delay when amendments are introduced to the security functions. These details will form the foundation of all inspections which are designed to assess the physical and logical security of the ATM.

OM-6.3.7 Banks are required to implement best industry practice in respect of hardware and software development and integration, including but not limited to formal specification, test plans, and documentation. Hardware and software should only be introduced to the environment following a successful programme of testing.

OM-6.3.8 All test plans and the outcomes of these plans must be retained by the bank for a minimum of five years from the date of testing and be available on request to the CBB or their authorised representatives. Examples of instances in which a detailed testing process must be undertaken prior to installation and integration of components include, but are not limited to, secure card readers or EPPs. In all instances the applicable standards relating to Payment Card Industry (PCI), PIN Transaction Security (PTS), and Point of Interaction (POI) requirements must be fully complied with.

OM-6.3.9 Banks must ensure that integration of the EPP, and any mechanisms which are designed to identify unauthorised activity within the ATM environment (such as removal of the ATM) are implemented in a timely and effective manner, and that such actions are in compliance with the standards and guidelines provided by the device vendor.

OM-6.3 ATM Security Measures : Hardware/Software (Continued)

OM-6.3.10 Banks must ensure that the ATM fasica (external body), cabinet design, and/or the physical positioning of the EPP do not facilitate the visual observation of PIN values as the cardholder is entering them. Banks must evaluate the extent to which a privacy screen and/or other visual observation deterrents (such as location of the EPP combined with defensive posture of the cardholder's body) facilitate compliance with these requirements and appropriate controls must be implemented to effectively mitigate the associated risks.

OM-6.3.11 Banks must ensure that ATMs are equipped with mechanisms to prevent or deter unauthorized transaction activity, or which is aimed at retaining and subsequent unauthorized recovery of the card by the perpetrators at a later time.

OM-6.3.12 Banks must ensure that ATMs are equipped with mechanisms to prevent or deter attempts to modify or penetrate the ATM to make any additions, substitutions, or modifications to the card reader or the ATM hardware or software. Examples of possible controls include, but are not limited to, the following:

(a) Compliance of the card reader to Evaluation Module 4 Secure Reading and Exchange of Data (SRED) of the PCI PTS POI Security Requirements; and

(b) The installation, where feasible, of two card readers (CRs) with segregated reading technologies (chip and magnetic-stripe).

OM-6.3.13 Banks must ensure that the integration of Secure Card Readers, (SCRs) and, if applicable, any mechanism protecting the SCRs are properly implemented and fully comply with the guidelines provided by the device vendor. SCRs must be approved by and fully comply with, all Payment Card Industry standards at all times.

OM-6.3.14 Banks must ensure that neither the logical nor physical integration of SCRs into the ATM creates any new attack paths to account data.

OM-6.3 ATM Security Measures : Hardware/Software (Continued)

OM-6.3.15 Banks must ensure that all ATMs, including offsite ATMs, are equipped with mechanisms which prevent skimming attacks. There must be no known or demonstrable way to disable or defeat the above-mentioned mechanisms, or to install an external or internal skimming device.

OM-6.3.16 Banks must ensure that anti-skimming devices are checked on a daily basis to identify any attempt to install unauthorized devices. To facilitate an effective control environment, a detailed check list must be developed and utilised, and all test results must be retained for a minimum of five years from the date of the test.

OM-6.3.17 Banks must ensure that each ATM is equipped with only one cardholder PIN-acceptance interface.

OM-6.3.18 In cases where the EPP can be used for non-PIN data entry, banks must ensure that there are effective controls in place to prevent unauthorised alteration of prompts.

OM-6.3.19 In cases where the ATM supports any input devices other than the EPP, including touch screens, banks must ensure that both the ATM display and additional input devices are securely protected to ensure that the input device is sufficiently secured to prevent the possibility of malicious abuse to capture Pins. All user interfaces must be protected against manipulation at all times.

ATM Software

OM-6.3.20 Banks must ensure that their ATM software security measures comply with the following:

a) ATMs perform an industry-standard self-testing routine upon startup, and at least once a day to check the software of the ATM Controller (AC) security mechanisms for signs of tampering with or compromising the ATM;
b) ATMs use and rely on EPP functions and control mechanisms for key loading and key management;

OM-6.3 ATM Security Measures : Hardware/Software (Continued)

c) Access to sensitive services is controlled by requiring authentication. Entering or exiting sensitive services must not reveal or otherwise compromise the security of sensitive information;

d) System generated limits on the elapsed time between physical inputs to the ATM are in place;

e) If an ATM supports multiple applications, it must enforce system generated separation between applications. It must not be possible that one application in any way compromises, interferes or tampers with another application or the Operating System (OS) of the ATM, including its ability to access, use, or modify data objects belonging to another application, even if they are distributed over separate components of the ATM;

f) ATM software must include controls which are designed to prevent unauthorised modification of the software configuration, including the operating system, drivers, libraries, and individual applications. Software configuration includes the software platform, configuration data, applications loaded to and executed by the platform, and the associated data. The mechanisms must also ensure the integrity of third-party applications, using a controlled process to install such controls;

g) OS and the software of ATMs contain the components and provide the services needed for the specific operation(s), or those that are protected under defined security policies. The OS must be configured and run on the basis of 'least required privilege' for each user. OS modules such as peripheral drivers, file systems, or inter-process communication protocols must be regarded as components. Applications responding to external interfaces must be regarded as services. Any applications which are directly required for the purpose of financial transactions must be removed, and all unused background services must be disabled;

h) Access to all elements of the ATM environment must be strictly controlled to ensure an effective segregation of functions and an effective segregation of responsibilities exists for all personnel;

OM-6.3 ATM Security Measures : Hardware/Software (Continued)

i) The ATM configuration must include a facility to log all ATM activity in real time, and retain details of such activity for a period of time as designated by the CBB from time to time. Logging activity and record keeping must be timely, accurate, and reliable. It must include, at least: activation of the service interface(s), all maintenance operations and physical access to the inside of the ATMs;

j) Adequate segregation of functions and effective segregation of duties are in place;

k) The logging data must be stored in a way that data cannot be changed under any circumstances, and deleted only after authorisation by a member of bank staff who has specific responsibility delegated by the CEO;

l) Access to the service interface(s) requires identification and authentication. Any remote service interface must be protected against information disclosure and intrusion;

m) During all periods when service functions are performed, ATMs must not perform cardholder transactions;

n) The communication interface(s) of the ATM must be protected against intrusion and misuse;

o) ATMs must incorporate dedicated tampering protection capabilities; and

p) All software updates must be incorporated in a timely manner.

Device Management/Operation

OM-6.3.21 Banks must ensure that their device management/operation controls comply with the following:

a) Change-control procedures are in place so that any intended change to the physical or logical capabilities of security-relevant components of ATMs are identified and appropriate measures taken in a timely manner;

b) Software is protected and stored in a manner which precludes unauthorised modification;

OM-6.3 ATM Security Measures : Hardware/Software (Continued)

c) Loading of software into ATMs is performed by a person who has the requisite knowledge and skills, and who has been nominated and authorised by a senior manager in the bank to undertake these tasks;

d) ATMs must be certified as fit for purpose by the manufacturer.

e) Software that is loaded to devices at the time of manufacture or deployment is transported, stored, and used under the principle of dual control, preventing unauthorised modifications and/or substitutions;

f) Upon delivery from a manufacturer or vendor, ATMs and all of their associated components must be thoroughly checked to ensure there are no signs of tampering with the packaging. Where unauthorised attempts to access the goods are identified, the ATM must not be commissioned;

g) The repair process and the inspection/testing process has not been subject to unauthorised modification;

h) ATMs' security-relevant components are protected from unauthorised modification with tamper-evident security features;

i) Documentation must be retained, both shipped with the product (the ATM and its related components and software). It must also be available securely online, including instructions on validating the authenticity and integrity of the ATM;

j) Each security-relevant device has a unique, visible identifier;

k) Upon decommissioning of an ATM all sensitive information and sensitive technical parts are destroyed in a secure manner;

l) Decommissioned ATMs must be stored in a secured area assigned specifically for the purpose;

m) All ATMs must prominently display a warning for customers to "protect and shield their PINs", informing them about skimming devices, providing general advice on ATM security, and details of a customer helpline to report incidents;

n) ATM screens must display how the unaltered ATM and card reader must appear; and

o) Procedural or automated controls exist to prevent the capture of cardholder account data in card readers used to access the area housing the ATMs.

OM-6.3 ATM Security Measures : Hardware/Software (Continued)

ATM Application Management

OM-6.3.22 Banks must ensure that their ATM application management complies with the following:

a) The ATM application must enforce in a secure manner the correspondence between the display messages visible to the cardholder, the operating system of the ATM, and the application the cardholder interacts with;

b) It must be obvious to the cardholder in 'clear' mode when the PIN-entry is required to be operated, when the PIN is being entered, and for which application;

c) ATM applications that are controlled or executed remotely use secure communication channels, and are authenticated throughout the execution process;

d) Cryptographically based controls are to be utilised to control the ATM display and ATM usage, so that it is not feasible for an entity not possessing the unlocking mechanism to alter the display and to allow the output of unencrypted PIN data from the ATM;

e) The entry of transaction data is separate from the PIN-entry process;

f) The display of a cardholder PIN on the ATM display must not be in 'clear' mode.

g) If other data and the PIN are entered on the same keypad, the other data entry and the PIN entry must be computer-controlled separate operations;

h) The transaction data transferred over the communication interface must be protected against unauthorized disclosure. If open channels are used, the data must be encrypted;

i) Sensitive information must not be present any longer or used more often than strictly necessary. The ATM must automatically clear its internal buffers when either the transaction is completed, or the ATM has timed out whilst awaiting a response from the cardholder or host; and

j) Prevent the display or disclosure of cardholder account information on the ATM screen, printed on receipts, or audio transcripts for visually impaired cardholders.

OM-6.4 ATM Security Measures: Physical Security

Implementation

OM-6.4.1 The requirements in this Section must be complied with in full within 6 months from the date of issuance. Failure to comply with any of these requirements will trigger a supervisory response, which may include formal enforcement measures, as set out in Module EN (Enforcement).

OM-6.4.2 Banks must implement effective controls to mitigate the risk of physical attack towards the ATM environment. Examples of such controls are outlined in the Appendix to this Chapter (Appendix – A).

Site Selection and Installation

OM-6.4.3 The installation of ATMs must always be preceded by risk assessments. During initial site validation, or at subsequent site risk assessment visits, an ATM must be classified by the deployer as low, medium or high risk. Risk assessment criteria can depend on organisational, insurance and law enforcement recommendations and requirements. As a minimum, such assessments must take account of:

(a) The safety of all staff, ATM users, and the public;
(b) The crime history of the area and the site, confirmed by local police intelligence;
(c) General conditions of the site, including lighting, proximity to other community services, and visibility of operation;
(d) The proposed positioning of the ATM within the environment of the selected site;
(e) Existing / proposed security measures on site;
(f) The cash replenishment model – bank staff, merchant or CIT crew; and
(g) The cash rating of the security container fitted to the ATM employed or to be employed.

OM-6.4 ATM Security Measures: Physical Security (Continued)

OM-6.4.4 Banks must record the details of the site risk assessments and retain such records for a period of five years from the date of the ATM installation, or whatever other period required by the Ministry of the Interior or the CBB from time to time, whichever is the longer.

ATM Deployment

OM-6.4.5 Banks must clearly define the party responsible for each of the following actions:

(a) The preparation of the site, including specified physical protection against "ram raids";

(b) The provision, installation, testing and commissioning of all security equipment;

(c) The installation and maintenance of a dedicated communication line/link (where applicable);

(d) The ATM Base preparation; and

(e) The installation and maintenance of all electrical wiring and the on-going provision of electrical power.

Installation

OM-6.4.6 Banks must ensure that contracts relating to ATM deployment clearly define the party responsible for the following actions:

(a) The installation, testing and commissioning of all security alarm equipment;

(b) The installation, testing and commissioning of all locks within the ATM environment;

(c) Defining and ensuring compliance with all general site requirements as designated by the Ministry of the Interior, the CBB and other appropriate bodies; and

(d) The provision of all plans/documentation relating to the construction of the building and ATM anchoring.

OM-6.4 ATM Security Measures: Physical Security (Continued)

Installation of an Off-site ATM in Bahrain

OM-6.4.7 **Applications for the installation of off-site ATMs must be sent in writing, and in accordance with the requirements set out in Paragraphs OM-6.4.9 to Paragraphs OM-6.4.16 to the Supervisory Point of Contact (SPoC), at the CBB.**

OM-6.4.7A The purpose of the content of Paragraphs OM-6.4.8 to OM-6.4.16 is to set out the minimum criteria to be followed by banks for the installation and usage of off-site ATMs in the Kingdom of Bahrain.

General Criteria

OM-6.4.8 **The ownership and operations of any off-site ATMs is subject to the prior written approval of the CBB and must comply with the Rules outlined in Paragraphs OM-6.4.9 and OM-6.4.10.**

OM-6.4.9 **Off-site ATMs must be owned either individually or jointly by retail bank licensees which are members of the BENEFIT Switch. Each relevant owning bank must already have linked its ATM capability to the BENEFIT Switch prior to requesting the CBB's permission to install an off-site ATM and, furthermore, must conform to the general standards set by the Benefit Company from time to time.**

OM-6.4.10 **Off-site ATMs must, be fully functioning or operate as cash dispensers only, at the discretion of the owning retail bank licensee.**

OM-6.4.10A In addition, off-site ATMs may, at each relevant owning bank's discretion, be 'walk-up' or 'drive-in' machines.

OM-6.4.11 **Owning retail bank licensees must bear full legal responsibility for their respective off-site ATMs, as well as all costs associated with such ATMs (including, but not limited to, cash replenishment, installation, security etc.).**

OM-6.4 ATM Security Measures: Physical Security (Continued)

OM-6.4.12 **Retail bank licensees wishing to install an off-site ATM must submit an application (in writing) for the CBB's approval (see Paragraph BR-5.3.3). A copy of the written permission (for installation of that off-site ATM) of the legal owner of the proposed location must be provided to the CBB, as well as a copy of the written permission of any other relevant authorities in this context (e.g. the Ministry of Interior).**

OM-6.4.13 The CBB will consider applications on a 'first come, first served' basis for a particular location. If more than one application is received to install an off-site ATM in the same location, the number of such applications which are approved will depend upon whether the location appears to the CBB to be capable of sustaining multiple off-site ATMs subject to the exact details of each individual application regarding security being acceptable to the CBB.

OM-6.4.14 Each application will be assessed on its individual merits, and at the CBB's sole discretion, taking into account factors which the CBB considers relevant including, but not limited to:

(a) The suitability of the location in question;
(b) The level of overall activities of the applicant in the market as well as the size and make-up of its customer base; and
(c) The type and range of facilities which the applicant proposes offering through the off-site ATM at the location in question.

OM-6.4.15 In addition to the information required by the CBB under Paragraph OM-6.4.12, the CBB may require further information/clarification to be provided to it before it takes a decision regarding the application. The CBB's decision in this regard will be notified to each relevant applicant bank in writing.

OM-6.4.16 **A bank must request in writing the CBB's permission to close any of its off-site ATMs.**

OM-6.4.17 The CBB may, at its sole discretion, require an off-site ATM to be closed and decommissioned at any time.

OM-6.4 ATM Security Measures: Physical Security (Continued)

Safe

OM-6.4.18 Banks must ensure that the level of security provided by the safe within the ATM is commensurate with that required for the maximum value of cash which can be loaded in the ATM.

Locks

OM-6.4.19 Banks must ensure that a time delay mechanism is fitted to the ATM, and that it operates effectively. The financial institution's security guard (Staff or third party) must be certified to operate the time lock effectively in accordance with the manufacturer's requirements. The time lock must then be connected to an appropriate alarm system with monitoring via an Alarm Receiving Center (ARC). (For details about Time Delay/Time Lock refer to the recommended locks OM-6.4.21).

OM-6.4.20 Banks must undertake appropriate tests to ensure the on-going operation of the ATM locks remains effective, and that such locks, as well as the related alarms, are functioning properly.

OM-6.4 ATM Security Measures: Physical Security (Continued)

OM-6.4.21 Banks must refer to the below table for the recommended locks:

Primary Safe Locking	The following locks are recommended: • A UL 437/Type 2, CEN Class B changeable key lock • A 3 wheel UL Group 2M/ CEN Class B Mechanical Combination Lock • A UL Type 1/ CEN Class B, 1 Time Code Electronic Combination Lock: in the event that this type of lock be used it is highly recommended that the following features should be taken into consideration: 1. Lock should support encryption technology for the codes 2. Unused lock codes should expire automatically 3. Seal code should start a security protection procedure in the event that the previous ATM closing has not been correctly effected 4. Lock should be able to provide Shared access between the Bank and the CIT company autonomously and simultaneously 5. That the owner of the lock can at any time be able cancel access to the ATM lock park without having to organise on site vendor meets • A UL Type 1/ CEN Class B Electronic Combination Lock If applicable, the electronic locks should be compatible with the monitoring/control system used by the Bank/ATM deployer.
Secondary Safe Locking (For dual control if required)	Where a mechanical 3-wheel combination lock is already in use, for the purposes of dual control an additional changeable key lock may be installed as a secondary lock to the primary. (A key locking dial may not be acceptable, dependent upon the agreed insured value for loss). Many modern electronic combination locks have a dual control function that allows dual control without the necessity to fit a second lock.
One Time Combination Locks (For Use With Approved Third Parties if required)	An approved third party is a commercial organisation authorised to carry cash in transit, to conduct cash replenishments and/or to conduct first & second line maintenance of the ATM. When such parties are used, it is recommended that one-time combination locks, with clearly identifiable audit trails, be used. Such locks may be used as the Primary Safe lock.
Time Delay/Time Locks	When required a programmable time delay lock may be fitted, allowing a pre-set delay whenever the lock is opened., this is usually 1-99 minutes in 1 minute increments Such a Lock, which may also be used as the Primary Safe Lock, may also be programmed as a Time Lock, whenever the Bank Branch/ATM Site is closed, and between replenishments.
Time Delay Override (TDO)	In the event that a Multiple/Dual User Electronic Lock is fitted, it should be able to be programmed with a Time Delay Override Code (TDO) that can be used by the CIT or ISO to allow the user to by pass the time delay for obvious reasons. The TDO should be able to be programmed to either allow direct after hours entry or Dual entry (second code needing to be entered within 60 seconds of the first)
Duress Alarm (Hold Up alarm)	The electronic lock should also be able to generate a "Duress" alarm. It is advisable that this code be easy to remember and use and not require any additional keystroke to activate. The best is 1 code up 1 code down activation; meaning if the code was 123456# the user would substitute the last digit by either a number above or below that of the last digit.
BPI (Bolt Position Indicator)	Electronic locks should also be able to provide a dry signal indicating if the bolt is in the Retracted position (open) or the Extended (Closed) position. This signal can be used to monitor the condition of the lock remotely, prevent a cascade (multiple door openings at the same time) attack on a group of ATMs or freeze the entry to the ATM room in the event that an ATM door is in the open condition. Alternatively there are many safe alarm systems in operation that monitor bolt position by other add-on means and these are acceptable and even compulsory alternatives in some countries.

OM-6.4 ATM Security Measures: Physical Security (Continued)

ATM Alarms

OM-6.4.22 In addition to alarming the premises, banks must alarm the ATM itself, in a way which activates audibly when the ATM is under attack. The system must be monitored by remote signaling to an appropriate local police response designated by the Ministry of the Interior. Banks must consider the following:

(a) If the alarm system is designed to confirm an attack, a dual signaling facility must be incorporated;

(b) The design of the ATM must ensure that the system is armed at all times other than during maintenance, servicing and cash replenishment;

(c) The design of the system must ensure that the ATM has a panic alarm installed;

(d) An alarm must be installed and functioning at all times which is immediately triggered when no card is inserted within a certain time limit;

(e) An alarm must be installed which is triggered when a customer touches certain spots of the ATM which are not typically touched for the normal services provided by an ATM;

(f) The design of the system must give an immediate, system controlled warning of an attack on the ATM, and all ATMs must be fitted with fully operational fraud detection and inhibiting devices;

(g) All members of CIT crews / ATM replenishment staff must be issued with effective personal attack alarms which can be easily activated in the event of an attack during cash replenishment;

(h) A maintenance record must be kept for the alarm detection system and routine maintenance must be conducted in accordance with at least the manufacturer's recommendations. The minimum must be two planned maintenance visits and tests every 6 months;

OM-6.4 ATM Security Measures: Physical Security (Continued)

(i) The alarm system must be monitored from an ARC 24 hours daily. It must automatically generate an alarm signal if the telephone/internet line fails or is cut; and

(j) In the event that an alarm signal is received, the ARC must respond according to its standard operating procedures.

OM-6.4.23 Banks must refer to the below table for the recommended alarm installations:

Seismic Detector / Stress Detector	A seismic / stress detector should be fitted to the ATM safe body and safe door.
Magnetic Contact	A dual reed magnetic contact switch should be fitted to the door of the ATM Safe. A dual reed magnetic contact should also be fitted on the door of the ATM Secure Service Room (if provided). This should be on a different circuit to the alarms fitted to the ATM safe.
Volumetric Detector	A volumetric detector should be placed on the wall of the ATM Secure Service Room. This should be able to detect any movement in the area surrounding the ATM. This should be on a different circuit to the alarms fitted to the ATM safe. If the Bank Branch has a cellar, which is under its direct control, a volumetric detector should be fitted to cover the area underneath the ATM anchoring.
Personal Attack Alarms	Personal Attack Alarms should be fitted in the ATM Secure Service Room as close as possible to the ATM. This is to provide protection to staff servicing or replenishing the ATM. If ATM's are in a public area, then consideration should be given to installing a radio based Personal Attack Alarm, such that staff can be issued with portable devices.
Alarm Control Panel(s)	An alarm control panel (combination) should be fitted in the immediate vicinity of the ATM where necessary. If access control is used to secure the room, then an additional panel does not need to be fitted at the room door.
Access Control	Where possible, access to the rear of the ATM should be restricted and a door swipe or keypad system should be used to control the ATM secure Service Room door.
Heat Sensor	A heat/smoke sensor should be fitted inside the ATM. This should detect any form of oxy-acetylene or burning bar attack on the ATM, and should be on the ATM security circuit.

OM-6.4 ATM Security Measures: Physical Security (Continued)

Closed-circuit television (CCTV)

OM-6.4.24 Banks must ensure that ATMs are equipped with Closed-circuit television (CCTV). The location of camera installation must be carefully chosen to ensure that images of the ATM are recorded, however keypad entry are not recorded. The camera must support the detection of the attachment of alien devices to the fascia (external body) and possess the ability to generate an alarm for remote monitoring if the camera is blocked or otherwise disabled.

OM-6.4.25 As a minimum, CCTV activity must be recorded (preferably in digital format) and, where risk dictates, remotely monitored by a third party ARC.

OM-6.4.26 When an ATM is located in an area where a public CCTV system operates, the deployer or agent must liaise with the agency responsible for the CCTV system to include the ATM site in any preset automatic camera settings or to request regular sweeps of the site. The CCTV system must not be able to view the ATM keypad thereby preventing observation of PIN entry.

OM-6.4.27 Banks must ensure that the specifications of CCTV cameras meet the following minimum requirements:

(a) Analogue Cameras:

Resolution – Minimum 700 TVL
Lens – Vari-focal lenses from 2.8 to 12mm
Sensitivity – Minimum 0.5 Luminance (Lux) without Infrared (IR), 0 Lux with IR
IR – At least 10 to 20 meters (Camera that detects motion)

(b) IP Cameras:

Resolution – 2 MP – 1080 p
Lens – Vari-focal lenses from 2.8 to 12mm
Sensitivity – Minimum 0.5 Lux without IR, 0 Lux with IR
IR – At least 10 to 20 meters

OM-6.4 ATM Security Measures: Physical Security (Continued)

OM-6.4.28 Banks must ensure that the following network requirements are met for connecting the Banks CCTV system to MOI Control room:

(a) The minimum speed of the upload should be 2 Mbps for each node (ATM's and branches);

(b) Speed/storage limit threshold must not be applied in a manner which permits a network delay; and

(c) Access must be restricted to authorised personnel.

ATM Lighting

OM-6.4.29 Banks must ensure that adequate and effective lighting is operational at all times within the ATM environment. The standard of the proposed lighting must be agreed with the Ministry of the Interior and other relevant authorities, and tested at least once every three months to ensure that the lighting is in good working order.

OM-6.4.30 In areas deemed to pose a higher risk to customers at night, CCTV camera must be fitted at floor level.

Anchoring

OM-6.4.31 Banks must implement the appropriate method of anchoring an ATM according the nature of the deployment and the perceived risk as identified through the risk assessment process.

OM-6.4 ATM Security Measures: Physical Security (Continued)

OM-6.4.32 Banks must refer to the below table for the different methods of anchoring an ATM:

Anchoring type	Description
Basic	The ATM must be securely fixed to the floor through its security container by a minimum of four resin anchor bolts (minimum 16mm diameter to a minimum depth of 150mm) into a substantial concrete base.
Base Composition	During the Site Validation an assessment must be made of the base to ensure that it is of sufficient strength and depth to anchor the ATM. It is recommended that screed is not included in any measurements of base depth.
On Solid Ground - Use Existing Base	If it is deemed possible to use the existing base, the existing concrete must be reinforced and of a minimum depth of 15cm to meet the requirements of the anchor bolt manufacturers. The ATM can then be anchored directly into it.
On Solid Ground - Plan for New Base	If it is not possible to use the existing base without modification, then arrangements must be made to strengthen the base. A minimum depth of 15cm reinforced concrete must be retained with the existing base, in order to anchor the new base to it.
ATM Plinth - Plinth Type Required	For the ATM to be properly anchored it must be able to sit on a plinth that will enable it to exactly reach the required height. When deciding on an ATM plinth, ATM deployers must assess its construction from a security perspective. Plinths specially constructed to withstand 'ram raids' and other brute force attacks may be considered for higher risk locations.
Anchoring ATM to Plinth	For installers using Central European Norm (CEN) approved plinths, the anchoring arrangements must be those that are approved in the CEN documentation for that product. The correct implementation of those arrangements will guarantee good anchoring.
7 Anchoring Plinth to Base - No Cellar – Sufficient concrete	This assumes that the ATM will be anchored into solid ground with sufficient concrete. Sufficient Concrete is reinforced concrete to a minimum depth required for the length of bolt used. For details of required depths it is recommended to consult the handbooks of the major anchor bolt manufacturers.
Anchoring Method - Installation Contractor	The installation contractor must anchor the ATM in accordance with the relevant CEN (or other) standard relating to the grade of safe used.
Anchoring Certificate - Installation Contractor	The Installation & Maintenance Contractor must complete a Certificate stating that the anchoring has been done in accordance with these requirements. All exact measurements relating to the anchoring must be recorded. A copy of this Certificate must be passed to the ATM deployer for audit purposes.
Anchoring Plinth to Base - No Cellar – Insufficient concrete	This assumes that the ATM will be anchored into solid ground with insufficient concrete. Insufficient concrete is concrete that is not reinforced and does not meet the minimum requirements of the anchor bolt manufacturers. When this is the case a concrete base must be constructed and properly attached to the existing floor.

OM-6.4 ATM Security Measures: Physical Security (Continued)

Solid Wall

OM-6.4.33 If accessible from an area with vehicular access, banks must ensure that ATMs are installed behind a solid brick or concrete wall. If one does not exist, it must be constructed.

OM-6.4.34 In order to comply with Paragraph OM-6.4.33, the wall must be at least 14cm thick and with a mass of 1,900 kg/m3. Any deviations from these requirements must be agreed with, and accepted by the ATM deployer and the Ministry of the Interior before installation of the ATM, and must be shown in the construction certificate.

Fire Alarm

OM-6.4.35 Banks must ensure that effective fire alarm and fire defense measures, such as a sprinkler, are installed and functioning for all ATMs. These alarms must be linked to the "General Directorate of Civil Defense" in Bahrain.

Cash Replenishment

OM-6.4.36 Banks must ensure that ATMs are not replenished during customer opening hours. Replenishment of off-site ATMs must be performed by specialised service providers, comprising a crew of at least two persons. All personnel, when replenishing an ATMs must carry a mobile phone or communication device in case of emergency.

OM-6.4.37 All cash movements between branches, to and from the CBB and to off-site ATMs must be performed by specialised service providers.

OM-6.4 ATM Security Measures: Physical Security (Continued)

ATM Service/ Maintenance

OM-6.4.38 Banks must ensure that all ATMs are properly maintained and that appropriate service or maintenance agreements are implemented. All ATMs must be inspected daily by bank staff to check that they are functioning properly and have not been tampered with. Any changes identified during these inspections must be documented and reported immediately to a designated senior manager at the bank. Where the ATM environment is reviewed and assessed as complying with all relevant security requirements, this must be verified by a senior manager at the bank accordingly.

OM-6.4.39 Banks must maintain a list of all maintenance, replenishment and inspection visits by staff or other authorised parties.

OM-6.5 ATM Security Measures: Additional Measures

OM-6.5.1 Banks may ensure the adequacy and effectiveness of external security measures throughout the ATM environment through the additional security measures outlined in this Section.

Banknote Degradation System

OM-6.5.2 Banks should ensure that a banknote degradation system is installed on each ATM cassette, where the money cassette sprays paint or chemical on the notes to stain/degrade/damage the notes and make them un-usable. The banknote degradation system should be designed to activate immediately when an ATM is moved or attacked by any means. If required, the system may incorporate a unique chemical identifying system, although such identification systems should be agreed with the Ministry of the Interior and should not be used in isolation. Where a banknote degradation system is utilised, notices to this effect should be displayed prominently around the perimeter of the premises and on the ATM itself.

Smoke Generating System

OM-6.5.3 Banks should ensure that a smoke generating system is installed on each ATM to protect the internal area of the premises. Such systems should be designed to activate immediately when an ATM is moved or attacked by any means. Activation should be programmed to occur only when the area of the premises in which the ATM is sited is non-operational. Such systems should not negate any procedures associated with fire and emergency, and they should not inhibit any means of escape in the case of an actual fire. Banks should ensure that advice is taken from the "General Directorate of Civil Defense" in Bahrain, and this advice is complied with before installation. Where a smoke generating system is utilised, notices to this effect should be displayed prominently around the perimeter of the premises and on the ATM itself.

OM-6.5 ATM Security Measures: Additional Measures (Continued)

Cassette Interlocking

OM-6.5.4 Banks should ensure the physical interlocking of cassettes is applied within the ATM safe, and that these are designed to prevent the removal of more than one cassette at any given time. A time delay between each cassette removal should be installed.

Sounders and Flashing Warning Lights

OM-6.5.5 Banks should ensure that street-based ATMs are installed with an audible alarm sounder, and a visual flashing warning light, to indicate when the ATM is under attack.

Bollards

OM-6.5.6 Banks should request the permission of the appropriate authorities to protect ATM sites by the installation of anti-ram raid bollards, vehicle arresting systems, high-rise kerbing, raised planters, reinforced lampposts or similar street furniture, usually subject to local authority approval, to prevent cars coming in high speed from colliding with the ATM and damaging it. Where such approval is provided, installation of the protection mechanism should be completed before commissioning the ATM.

Armored Anti-Bandit Shroud

OM-6.5.7 Banks should obtain and act upon advice provided by the Ministry of the Interior in respect of protecting the ATM installation with an armored anti-bandit shroud which is placed around the ATM to prevent any bombing or other physical attempts to damage the ATM.

OM-6.5 ATM Security Measures: Additional Measures (Continued)

Servicing of ATMs

OM-6.5.8 Servicing an ATM should be undertaken by a suitably certified service engineer. Where an armored anti-bandit shroud is not being used, banks should ensure that "cash in transit services" are used to secure the ATM cassettes throughout the servicing process.

Defensible Space

OM-6.5.9 Wherever possible, banks should specify a "Defensible Space Ground Marking" zone in front of each ATM, to ensure that only one customer at a time is allowed to enter the space.