

Annex 2

**OPERATIONAL RISK MANAGEMENT PRINCIPLES FOR INFORMATION
SYSTEMS IN FINANCIAL INSTITUTIONS**

Contents

INTRODUCTION	2
A. ORGANISATION AND MANAGEMENT OF IT SYSTEMS	3
A1. IT GOVERNANCE.....	3
A2. INFORMATION SYSTEMS DEPARTMENT ORGANISATION.....	5
A3. RELATIONS WITH TECHNOLOGY SERVICE PROVIDERS	5
B. DEVELOPMENT AND ACQUISITION	8
B1. SYSTEMS DEVELOPMENT	8
B2. SYSTEMS ACQUISITION.....	11
C. PRODUCTION AND SUPPORT	13
C1. SYSTEMS OPERATION	13
C2. PHYSICAL & ENVIRONMENTAL SECURITY	15
C3. LOGICAL SECURITY	16
(α) for the systems access security:	17
(b) for the data security:.....	18
(c) for the systems security:.....	19
(d) for the network and telecommunications infrastructure security:.....	19
C4. BUSINESS CONTINUITY & DISASTER RECOVERY PLANS	21
D. INFORMATION TECHNOLOGY AUDIT	23

INTRODUCTION

The Bank of Greece, in the context of its supervisory powers/ as the authority responsible for the supervision of the credit system, attaches particular importance to the secure and effective operation of the Information Technology (IT) systems of Financial Institutions (FIs). The first set of rules and guidelines for IT systems was introduced by Bank of Greece Governor's Act no. 2438/98. The present document lays down a more detailed and structured framework of general principles aimed at ensuring the secure and effective operation of IT systems, while at the same time taking account of the most recent developments in IT insofar as they have a bearing on the operation of FIs. This set of principles will also serve as a basis for the supervisory evaluation of FIs in this particular area.

Such set of rules and principles should contribute considerably to the effective management of Operational Risk inherent in IT Systems. This need is also dictated by the new capital framework of the Basel Committee of Banking Supervision (BCBS), commonly known as "Basel II", framework, which for the first time introduces operational risk into the calculation of credit institutions' capital requirements.

These principles can be classified in four categories, namely:

- *Organisation and Management*, referring to IT Governance, the organization of the IT function/business area and relationships with vendors;
- *Development and Acquisition*, referring to standards, procedures and methodologies for the development and acquisition of IT Systems;
- *Production and Support*, referring to operational procedures, IT physical and logical security and business continuity;
- *IT Audit*, referring to the rules and essential requirements for the efficient and effective operation of IT Audit

A. ORGANISATION AND MANAGEMENT

A1. IT Governance

Information Technology Governance is a part of Corporate Governance and falls within the responsibility of the Management of a FI. It encompasses all the complete business structures and procedures designed to ensure that the IT Division supports the strategy and goals of the FI; adds value to the organization, manages efficiently the resources allocated to it; evaluates and manages effectively the risks that arise from IT systems; strictly complies with the Information Security Policy; is able to use a set of control mechanisms in the context of the FI's overall control framework.

In order to achieve the above mentioned goals, the FI must:

1. have put in place an approved IT strategy that is consistent with the FI's overall business strategy. The IT strategy should, on the one hand, pursue the business goals set by the Management and, on the other, develop the necessary technological infrastructure to accommodate for the future needs of the organization. The FI must have the proper business units and procedures for the creation of the IT strategy, its observance and for its continuous maintenance in order to keep the strategy always on the path of the overall business strategy and of the country's legislation. The IT strategy must include short-term and long-term plans.
2. have an IT Steering Committee, comprising executives of the FI and preferably headed by a member of senior management with knowledge in the field of Information Technology. The mandate, tasks and composition of the committee must be laid down in an official regulation. The tasks of the committee shall include the following:
 - evaluation of short- and long-term IT planning against the overall business plans
 - evaluation of IT risk analysis and management;
 - evaluation and approval of large-scale procurement contracts for hardware and/or software;
 - monitoring of large projects and of the IT budget
 - setting of priorities;
 - approval of policies, standards and procedures;
 - approval and monitoring of relationships with vendors (e.g. for outsourcing).

The committee shall always receive a copy of the audit reports regarding the IT systems.

3. have a Risk Management Unit (RMU), which will evaluate, categorize and manage the risks that arise from the development, integration and use of IT systems; such risks must always be assessed along with all the other risks faced by the FI.
4. have a documented Security Policy for the IT systems, approved by management in the form of guidelines and principles that prescribe the direction and the goals of the FI towards an effective management, protection and distribution of IT resources.
5. have beyond the Security Policy the proper management structure and hierarchy that will guarantee the security of information in the Financial Institution. Based on this structure, the FI must envisage the position of a Information Security Officer (ISO) whose independence and impartiality must be ensured by having the ISO report directly to senior management.
6. ensure that all the policies, procedures, standards and methodologies documented and approved by the appropriate body within the Financial Institution.
7. have standards and methodologies for the design, development and operation of Information Systems.
8. have standards and methodologies for the management of IT-related projects.
9. guarantee the quality of the provided IT services through quality assurance procedures as part of the FI's Total Quality System. Quality assurance shall must be guaranteed in every part of the Information Technology Systems life cycle and cover the deliverables, documentation, training, specifications, procedures and project deployment plans.
10. have appropriate procedures for the timely detection and effective dealing with problems that arise from the operation of IT Systems.
11. have procedures for the detailed event type logging and classification of operational risk that originates from incidents in information systems and for reporting to the appropriate business units. The recording of incidents must be systematic in order to create historical data, and detailed so that the incident can be described accurately. The information should be kept in electronic form and be structured in such a way as to allow automatic report creation and transmission.
12. have a Management Information System (MIS) for the efficient reporting to the management. The MIS should ensure uniform and standardized collection, and processing, timeliness, accuracy, reliability and completeness of the information

presented to users. Data collection and processing should be as automated as possible.

13. be cognizant of, and comply with, the IT related legal, supervisory and regulatory framework.
14. study, evaluate and apply, where appropriate, the international standards and best practices for the secure operation of information systems, and keep abreast of technological change in these fields .

A2. Information Systems Department Organisation

The Financial Institution must have a specialized IT Department, operationally and administratively independent from the end users of IT services. The IT Department must:

1. have an organizational chart, which:
 - will reflect the organizational and business needs of the IT Department and clearly define the responsibilities of individual divisions or units;
 - provide a clear representation of the segregation of duties in order to prevent incompatible roles and ensure accountability, and optimum use of human resources. This would involve in particular a clear-cut segregation of duties between the area responsible for the analysis, design and development of information systems and the area responsible for the day-to-day operation of IT systems
 - an Information Systems Security Unit depending on the size and the information systems complexity of the Financial Institution. This unit works closely with the Information Security Officer in monitoring the information systems level of security and the risks arising from the development, introduction and operation of information systems. Their responsibilities include participation in the analysis and evaluation of IT risk, the formulation and maintenance of the Security Policy, identification and addressing security gaps and dealing with emergency situations
 - ensure staff replacements at least for the most critical operations
2. have documented and officially approved job descriptions, specifying the responsibilities, qualifications and skills required for each position.

A3. Relations with Information Technology Service Providers

When the Financial Institution cooperates with vendors (e.g. information service providers) on IT issues, it should take consideration of the following:

1. Using vendors can help resolve significant problems that would be hard to address otherwise. On the other hand, it can be a source of additional risks to the FI; such risks need to be identified, evaluated and effectively addressed/managed. The risks involved by outsourcing include the following:
 - lack of effective control over the offered services
 - increased dependence on third parties
 - loss of business knowledge/failure to develop an in-house know-how
 - potential failure to immediately respond to customer needs and market conditions
 - the black box approach of the vendors on costing issues
 - the FI's own staff resistance to outsourcing
 - the different culture between the Financial Institution and the vendor
2. If the FI chooses to outsource part or whole of the IT services, proper procedures should be in place for:
 - the evaluation of the risks entailed by outsourcing
 - the vendor selection process
 - the contract completeness and accuracy
 - the security and efficiency supervision and control of the vendor's information systems
3. The outsourcing of vital Information Systems for the Financial Institution must be justified in writing by the IT Steering Committee and officially approved by senior Management.
4. During the vendor selection process, further to the evaluation of the services provided by the vendor, the vendor himself should also be evaluated in terms of the following, also depending on the size and criticality of collaboration:
 - the financial soundness and long term viability
 - the impact of the contract on the vendor's business/turnover
 - reputation, client list and satisfaction
 - organizational structure (hence, ability to provide effective support to the offered services)
 - the adequacy (in terms of quality and quantity) of personnel assigned to the job
 - insurance coverage, etc.

In cases where the vendor uses subcontractors to perform parts of the contract, such subcontractors must also be evaluated, using the same criteria as for the original vendor

5. From a technical point of view, the vendors must be evaluated in terms of:

- the existence and quality of their Security Policy;
- the reliability of their systems;
- the suitability of the applied technology;
- the completeness of service support procedures;
- business continuity and disaster recovery plans.

The findings of internal or external auditors regarding the vendor, if available, constitute valuable input for the selection of vendors.

6. The contract to be signed must specify, among other things, the following:

- the rights and obligations of the contracting parties
- the service level agreement(s) and pricing policy
- the possibility of and procedures for renegotiating the contract
- ownership, licensing, and copyright clauses
- clauses on subcontracting
- the dispute resolution procedures
- the contract termination procedures (e.g. Escrow Agreement)

Specific mention should also be made to the following:

- information security (confidentiality, integrity, availability and traceability);
- contracting parties certification and non-repudiation;
- penalty clauses in the event of default
- the right to audit the vendor's premises (e.g. in case where a critical system to the FI is located at the vendor's premises)
- the right of the FI to assign to a third party the audit the vendor's premises
- the type and frequency of reports to be exchanged between the two parties
- the vendor's disaster recovery and business continuity plans

B. DEVELOPMENT AND ACQUISITION

A system's life cycle shall be divided into distinct phases, in line with standards, methodologies and procedures as established in writing. These phases are the Feasibility Study, Business Requirements Analysis and Specification, Technical Analysis and Design, Development, Testing, Acceptance and Transfer to Production, Operation and Support and Retirement. Transition from one phase to the next takes place only after the previous phase has been completed and its results have been reviewed.

The oversight of the project for the development of any crucial system must be assigned to the IT Steering Committee. Once the project has been completed, the day to day running of the new system and its operational and technical supervision must be assigned to the relevant/competent functions.

Before the development or acquisition of any mission-critical system for the FI, a Feasibility Study shall be required. During this phase, the aspects of the new system to be examined include definition of the new system functionality; cost/benefit analysis (reduction of current cost, increased profitability, improvement of the FI image); availability of requisite human resources and hardware/software; and, finally, evaluation of the cost of internally developing, operating and supporting the new system compared with the cost of purchasing a complete system or outsourcing the development.

B1. Systems Development

If the FI chooses to develop an Information System internally/in-house, the following must apply:

1. Before the start of the new system development, a Project Team must be set up that will create a project plan and manage the entire project. The Project Team depending on the size and the importance of the system must have as members the project leader, the security specialist, designers/ programmers, and representatives of users or other parties involved.
2. The project plan must specify in detail the project phases, their duration, the persons responsible for the completion of each phase and the respective deliverables. Also, the project plan must specify the lead times for the delivery of hardware or services by third parties, insofar as they can affect the time scheduling of the project.
3. A communication plan must be created, specifying procedures for: project status reporting to all parties involved; communication of issues requiring management attention; communication between the Financial Institution and vendors; and for announcing the changes and their impact on the organization.

4. the FI should consider matters regarding the acceptance and effective operation of the new Information System from the FI employees and adopt a change management plan in order to cope with potential negativity on the part of users and ineffective customer service due to poor familiarization.
5. The information gathered during the Analysis of Business Requirements and Define Specifications phases should be relevant to the concerns and requirements, as identified by the users themselves and the improvement needs that the users have located regarding the existing system. The requirements should define *what* the new system should do and not *how* and the specifications should define in general terms how the users requirements are to be implemented. The level of cooperation between the legacy systems and the new system must be examined during the new system requirements definition phase.
6. perform a data sizing and a total transactions count for the new system taking under consideration the current and the future needs in order to pinpoint with the greatest accuracy the new system hardware requirements and matching specifications.
7. proceed with a detailed management plan for the system or non-system legacy data that will include aspects such as data cleansing, data conversion in a form to suit the new system and data migration from the old system to the new.
8. during the phases of Technical Analysis and Design, a thorough risk analysis should be performed in order to define in detail the system secure operation requirements also in line with the security policy of the FI, the system security technical requirements (which include among other things the specification of the system's logical security parameters), and finally the system data control and reconciliation functions along with the structure of the necessary audit trails and logs according to the European Commission's "The Use of Audit Trails in Security Systems: Guidelines for European Banks". During these phases, cooperation with the Internal Audit function is deemed necessary so that they can recommend the proper controls and audit trails and logs that must be produced to facilitate the audit process. This cooperation shall not in any way interfere with the audit work performed by the Internal Audit Function for the system.
9. The system development must take place in an IT environment separate from that of the production and must comply with the common standards established by the FI (e.g. use of specific tools and methodology for the system development) in order to achieve a homogeneous and easily supported IT environment.

10. System tests must be performed during the first phase by the IT personnel in a separate environment and with predefined scenarios. The second phase must include complete and documented tests that include:
 - recovery testing, aimed at assessing the system recovery capability in case of software or hardware failure;
 - security testing, aimed at verifying that the system incorporates the appropriate security controls as specified in the system design;
 - stress testing, involving simulation of the system's performance under conditions of large volume of data processing

These tests must be attended, in addition to the programmers, by the Quality Assurance function (where available), the Security Officer and the Internal Audit function.

11. The system acceptance tests must be thorough and complete and take place in an environment that simulates as close as possible the production environment. Where the new system is intended to replace an existing system, the two systems must operate in parallel (parallel run) for a pre-specified period of time so as to enable comparative performance assessment. The participants in the said tests, once they have reached a decision on the system acceptance or otherwise, shall communicate it in writing.
12. The transfer of the new system to production should be undertaken by authorized personnel only (e.g. librarians) based on documented procedures, in a time period when no other important projects are under way and taking precautions to ensure that in an emergency situation the system can be brought back to its previous condition.
13. The system, before becoming operative, should have complete manuals that meet the quality standards set by the FI. The manuals should have a common format and structure.
14. System training for the users should take place in a separate IT environment other than the development and production environments. The training environment should remain active at all times, as an alternative to be used in cases when the production system is undergoing changes.
15. System operation and support should include procedures for systems change control, versioning, systems update and patches handling, system performance control, data and system backup, business continuity, help desk update to enable constant user support, etc.
16. The system retirement phase should include procedures for the preservation of information according to statutory and regulatory requirements, media sanitization of critical information, and hardware and software disposal. During this phase it is of the utmost importance to ensure that any systems connected

with the system being withdrawn are capable of continuing their normal operation.

B2. Systems Acquisition

If the FI decides to acquire an Information System, the following, additionally to the above, must apply:

1. The process of Information Systems procurement must be divided into distinct phases, each being subject to specific and approved standards, methodologies and procedural steps. Such phases are the Request For Proposal (RFP), whereby the FI provides a detailed description of its requirements for the new system, the vendor selection, the agreement and contract signing, the introduction of the new system into production and, finally, the system management and control.
2. The selection of the new system must be based on: its conformity with the detailed requirements specified by the FI; its expansion and adaptation capabilities in view of ever-growing business needs; its user friendliness; security aspects (logical security, audit trails & logs); level of support; reporting system etc.
3. The type of the parameterization that the FI will have on the acquired system must be strictly defined beforehand. Any interventions should follow approved and documented procedures, be applied by specialized personnel and be kept to the minimum required for safeguarding the identity and structure of the original system and the easy update and maintenance of the system. It is worth noting that in the event of major divergence between the FI operations and the functionality supported by the new system, the FI will typically have to adjust its operational procedures to the functionality of the system and not the other way round.
4. In centralised banking systems, the development of peripheral applications that will retrieve data from the central system and respond to local or business-specific needs must take place according to the FI's programming standards in order to ensure information systems homogeneity.
5. The systems external support function must be strictly predefined, with a clear specification of the cases when external support is required along with the respective response times.
6. The provision of remote access support on the part of the supplier should be limited to a small number of clearly defined cases and be treated with extreme caution, and all the supplier's actions must be logged for control purposes.
7. A transfer of know-how must take place not only through proper training of the staff involved in the running of such information systems but mainly through

their participation in each and every stage of development and parameterization of the system in order to gradually diminish dependency on the supplier.

8. When all the requirements – according to the contract – of the FI have been met and after the completion of the necessary tests performed by the supplier, a procedure should exist for the formal acceptance and delivery of the system from the supplier to the FI with attendance of all relevant parties.

C. PRODUCTION AND SUPPORT

The smooth operation of the Information Systems and their effective support and maintenance are crucial both for the normal operation of the FI and for building trust relationships with customers, as well as for effectively dealing with operational risk. They presuppose the existence of standards, policies and procedures and compliance with them by all involved FI business units and outsourced vendors.

C1. Systems Operation

The term "Systems Operation" includes all the procedures required for the day to day operation of Information Systems in a Financial Institution. In order for the Information Systems to effectively operate with an acceptable level of security, the following must apply:

1. Complete and detailed documentation of the hardware (main systems, servers, PC's, peripheral devices, networks and telecommunications), the architectural design, and of the software and its versions, updates, patches and licenses. A log must be kept for all the media that store and transport sensitive data (cartridges, tapes, floppy disks, CDs, printouts, microfiches). The log must be updated immediately when a change takes place.
2. Complete and detailed documentation for every Information System (hardware and software) that must include the official vendor manuals along with any manuals prepared by the IT staff for the day to day operation and maintenance of the Information Systems.
3. Efficient and effective maintenance and technical support of the Information Systems, in line with the vendor's guidelines and specifications and the everyday run requirements.
4. Support to staff users inside the organization and customer users outside the organization (e.g. e-banking customers) must be assigned to properly organized and specialized units such as the Help Desk. During the support phase, the type of users and the nature of the problems faced should always be taken under consideration. Data on the incidence and type of problems should be recorded and statistically processed.
5. Procedures for the management of system operational parameters.
6. Procedures that will prevent the installation and use of illegal, non- authorized or non-licensed software.
7. Scheduling of the tasks to be executed, recording of any problems arising and of the actions to be taken in emergency situations. The execution or non-execution of scheduled and/or ad hoc tasks should be recorded in a special log signed by

the staff involved in the execution of tasks. The execution of ad hoc tasks shall require prior approval.

8. Data control in order to ensure their integrity, validity and confidentiality during all phases of their processing cycle. Discrepancies of any kind should be identified and addressed in accordance with documented procedures.
9. Procedures for the systems and network monitoring of capacity, load and performance.
10. Continuous monitoring of information systems and network availability. Especially for critical systems, the FI must be able/in a position to calculate a availability rate in annual percentage terms and compare it with the defined targets. Furthermore, the FI must have procedures for the detailed documentation of the non-availability incidents (affected systems, non-availability elapsed time, cause of the problem, method and time frame of addressing the problem, frequency, cost to the FI), and for immediate notification to the responsible organizational units (Internal Audit, Risk Management) and top Management.
11. Adequate procedures for data and system backup handling (a more detailed approach to the subject can be found under Chapter 4).
12. Especially for the e-Banking Information Systems, the following must also apply:
 - i. The FI shall ensure that its website provides sufficient information to its potential customers, before they make any electronic transactions, regarding the FI's identity and its licensing authority . Additionally, the website must provide contact details of the support department in case any problem arises, the digital certificate of the website which must have been issued by an official certification authority, rules and guidelines for the secure operation and use of the offered services etc.
 - ii. The FI shall provide information about its privacy policy in respect of customers' personal data. It is recommended that such information be disclosed via the FI's website. Also, the FI shall give customers the option to deny the transfer of their personal data to third parties for advertising or other purposes. Customers' personal data may only be used for the purposes for which they were originally collected
 - iii. The FI shall make it clear to customers whenever the hyperlinks contained the in its e-banking website redirect users to websites of other companies or institutions and ensure that customers are aware that by following such links they are entering the website of a different business firm/corporation or legal entity.
 - iv. The FI shall ensure that automated transaction monitoring systems are in place, including historical data on service usage patterns and customer

profiles that will help detect and record any unusual transactional behaviour and generate, in real time, alerts for possible cases of fraud.

- v. The FI shall ensure that adequate mechanisms are in place for the effective management of the risks associated with money laundering and the financing of terrorism. These risks are particularly high in e-banking due to the service's ease of use irrespective of time and/or place, the impersonal nature and automated completion of transactions. For this reason, the FI should cater for the installation of automated filters and monitoring systems and tools for the managing of transactions that will set limits on certain groups of users or types of transactions and have the ability to withhold the execution of a transaction until the verification of certain information.
- vi. The FI shall ensure that easily retrievable historical records of past transactions are kept, enabling the detection of unusual transaction patterns and/or irregularities and the collection of information and reporting to the supervisory authorities, especially in cases of fraud, money laundering, investment services etc.
- vii. The FI shall make manuals in electronic or hard copy form available to customers, with instructions on secure e-banking. and secure use of personal computers through which e-banking and e-payment systems can be accessed. Such guidance should also contain best practices for protection from viruses and other malicious software, safe data storage, and use of personal user names and passwords (especially in shared computers, the use of which for these purposes should be generally avoided).
- viii. The FI shall ensure that effective security procedures are in place, with emphasis on accreditation of the communicating parties (digital certificate for the website of the FI, two-factor authentication for customers, T.A.N. lists or other methods), non-repudiation of transactions, message encryption, security of transactions (successful completion receipt, disconnection of an inactive user, detection of suspicious transactions etc.) and finally the operation of the systems that support the e-banking services in special areas of the network that are highly protected from malicious acts by internal or external users.

C2. Physical & Environmental Security

The term "Physical and Environmental Security" refers to measures taken to protect IT systems and infrastructure from various environmental risks. Before such measures are taken, a risk analysis is necessary, since physical security requirements may vary both across locations and within a given location depending on the criticality of the systems concerned.

The physical and environmental security measures must at least include:

1. physical access controls that restrict, control and monitor entry and exit of authorized personnel and visitors along with the transportation of infrastructure and storage media. Physical access controls should exist not only in areas where IT infrastructure is located but also in areas that house cabling of critical systems, supporting devices (UPS, alternative power generators), backup media etc. The existence of physical access controls should not cover only the Machine Rooms but extend to areas the Financial Institution characterizes as critical (branches and local divisions IT systems). The type of controls to be applied must be chosen on the basis of the criticality of the respective systems.
2. mechanisms for controlling potential physical hazards (fire, water damage etc.)
3. mechanisms for protection from malicious acts (breaking in, theft, vandalism, terrorist act etc.). These risks, as well as the risks mentioned in the previous paragraph, can cause total destruction of the systems and network infrastructure and jeopardize personnel lives.
4. mechanisms for the prevention and resolution of problems caused by a disruption of operation and supply of services or of a failure of supporting devices. It is necessary that the systems operate in a technically efficient environment.
5. effective management of the telecommunications and network cabling in order to prevent cases of wear, interference and lack of proper annotation.
6. security mechanisms for mobile information systems. The use of laptops or any other mobile information systems should be seriously taken under consideration during risk analysis. Laptops that store sensitive company data should from on the one hand be kept in a safe place when not in use and on the other store the sensitive company data in an encrypted form.
7. the safe transfer and storage of sensitive documents and magnetic media. The classified reports, the administrator's backup user names and passwords, the envelopes with the clients passwords to be dispatched, the systems and applications manuals, the Disaster Recovery and Business Continuity plans belong in the first category. The second category includes backup tapes, credit/debit card blanks etc.
8. the selection and proper arrangement of the area in order to minimize physical and environmental risks, taking account of the future use and the criticality of the systems.

C3. Logical Security

The term "Logical Security" refers to a set of measures and controls designed to restrict access to the system resources, i.e. hardware, network equipment, software

and data. Logical security measures define not only “who” or “what” (e.g. a programme) will have access to specific system resources but also the type/extent of access permitted . These measures can be embedded in operating systems, application software, databases, network management systems or be implemented through additional security modules.

In order to achieve an acceptable level of security, the following must apply:

(a) for :

1. users must have a unique user account for access to each system and only for the resources available to them, so that each and every movement can be logged for a particular person in order to ensure accountability. Therefore common/group accounts should be avoided and, when this is not possible, the transactions and system movements of these accounts users must be logged and reviewed frequently and carefully.
2. documented and approved procedures must exist for user account management and the definition and revision of user account rights for all the stages of a user's working life (recruitment, transfer, change in tasks/job description, termination of employment). A segregation of duties must apply to the processes of approval, activation and control for each user account.
3. the transactions and system movements of accounts with privileged information such as administrators and system owners must be logged and reviewed frequently.
4. user accounts must be deactivated immediately as soon as they stop being necessary or in case of a serious breach of security.
5. a detailed procedure must have been established that will allow for the creation of temporary user accounts with a predefined level of authorization to be used for special jobs or cases of emergency. The use of these accounts should be monitored closely and controlled and should be exist on a "need to have" basis.
6. the owner of a system user name must be authenticated during the system log-in process through a highly secure procedure (e.g. using a password, smart card, digital certificate etc.).
7. the original passwords that have been assigned by the vendor should be changed immediately after the delivery of the system.
8. passwords should:
 - be created and managed in accordance with documented procedures and standards;
 - be hard to guess;
 - be kept secret at the responsibility of their respective owners;

- be changed on a regular basis and definitely on the first sign on of the user to the system. Password change should be mandatory by the system and, where possible, a password history should be kept in order to prevent the repetitive use of the same passwords
- 9. backup passwords of the system administrator's or advanced rights users should be kept in a safe place, so that they can be used, based on a special procedure, in case of emergency.
- 10. where deemed necessary, passwords to special user rights accounts should be divided into several parts which are kept independently at the responsibility of different persons.
- 11. where possible, special software for user access management and control should be used.

(b) for data security:

1. Efficient and effective embedded data controls should exist in the various systems focused on the preparation, input, and processing of data.
2. A documented and approved classification of data according to their level of sensitivity should be in place, with additional security procedures envisaged for sensitive data through encryption or other means of protection.
3. With particular regard to cryptography, the following must apply:
 - the occasion and level of cryptography must be determined in detail;
 - a high level security key must be used at all times;
 - a public key infrastructure must be developed for the management of digital certificates mostly for communication between the FI its customers in the context of e-Banking;
 - the FI must always aim to comply with the national and international regulations and practices regarding cryptography.
4. The necessary actions should be taken to ensure compliance with the relevant provisions of Data Protection legislation.
5. A policy should exist to ensure that customers are informed of any leak of personal data due to a breach of systems security.
6. For the databases:
 - complete and detailed documentation of the database should exist that must include at least the logical and physical design and the data dictionary;
 - reindexing of the database should be performed on a regular basis;
 - a commit and rollback function should exist for the data to be used in case of emergency

(c) for system security:

1. At least in the critical systems and wherever else is deemed necessary, antivirus software or other protection against malicious programmes. The protection software must be updated regularly and installed in such a way as to allow for its automatic activation and update and to disallow uninstalation of the application/tool by users. The system properties must only be changed by the administrator.
2. Effective protection should be ensured for sensitive system resources such as system and application files.
3. A log must be created with the software approved by the Financial Institution.
4. Any system software or module that is not deemed necessary by the FI must be uninstalled or deactivated.
5. At least the basic auditing and logging functions in every system should be activated and parameterized properly with the assistance of the Internal Audit function.
6. It must be ensure wherever necessary, following proper and documented approval procedures, that the systems and other software are continuously updated with the latest security updates and patches in order to minimise their weaknesses and vulnerabilities.
7. Documented secure system restoration procedures must be in place, to address cases of a breach of security.
8. Where possible, the e-mail should be protected from spoofing attacks, theft or content alteration, dangerous attachments, spam mail etc.
9. The actions performed by system users via the Internet should be restricted (for example, access to specific websites, file transfers etc).
10. Users must be constantly trained and updated on systems security.
11. It must be ensured that the critical systems are effectively protected from malicious acts either by internal or by external users. To this end, a number of techniques should be applied such as:
 - the use of specialized software (firewalls, filtering routers etc.) which, acting as gatekeepers, will manage and control communication to and from areas of the network that are typically exposed to increased risk;
 - the creation in the network of specialized areas (Demilitarized Zones – DMZ) between access control points that will operate as a stand-alone network for FI systems accessible by internal or external users, in order to protect effectively the rest of the network from malicious acts.

(d) for the network and telecommunications infrastructure security:

1. Gateways with external networks must be clearly defined, documented and controlled.
2. The segmentation of the network into several small controllable subnets should be considered.
3. Care should be taken that all ports in every network device are closed, except for the ports that are necessary for the operations they support, also taking account of the risk entailed by their operation.
4. Access to special network administration and control mechanisms must be restricted and monitored effectively.
5. There must be an effective management of the parametrization of the network devices.
6. The network administrator must be able to locate unauthorized devices that operate within the network.
7. Physical access points to the network that are located in non-controlled areas should be kept at the absolutely necessary minimum and be deactivated when not in use.
8. The possibility of wireless access of users to the network should be limited and controlled periodically in order to avoid intrusion by unauthorized users.
9. Remote access to the network should be restricted; when such access is necessary, it must be logged and controlled periodically. In the particular case of dial up remote access, the system must provide for a "hang up/call back" process or another method of caller ID verification.
10. Proper communication protocols should be used, depending on the type of data transferred, thus addressing effectively data management and security issues.
11. The confidentiality and integrity of the data transmitted through the network must be safeguarded all along their journey.
12. Specialized software tools should be used in order to detect any security vulnerabilities or low security points within the network (vulnerability tests).
13. Procedures and specialized software should be used for the surveillance, avoidance and management of intrusion attempts to the network or general attempts to bypass the network security (intrusion detection / prevention systems).
14. Penetration tests should be conducted on a regular basis by specialised companies, based on predefined scenarios in order to evaluate the effectiveness of the network security.

C4. Business Continuity & Disaster Recovery Plans

Financial Institutions must have Business Continuity Plans (BCP), approved by the Management, for Information Systems as part of the FI's Global Business Continuity Plans in order to ensure the continuity of the business functions in case of a disaster. The Financial Institution must additionally have efficient and effective Disaster Recovery Plans (DRP) to be applied in cases where due to a disaster there is a critical system failure or a shutdown of the entire Computer Center.

Before the creation of the BCPs and DRPs a business impact analysis and a risk analysis must take place in order to:

- define all the critical functions and the systems/resources that support them;
- define all the risks that threaten the critical functions and categorize them according to their probability and potential implications;
- estimate the business cost in case of critical systems or functions shutdown and the BCP or DRP activation cost in order to define what parts of the plan must be activated and under which circumstances
- define the recovery time of the critical systems/functions along with the recovery point thus specifying the required systems recovery time and their exact position.

The first level of business continuity can be achieved through a backup plan for the software, the system parameters and the data and through backup/contingency equipment, UPS and power generators in the computer center.

In order to achieve fast and successful data and systems recovery the following procedures must be included in the backup plans:

- backup creation with frequency depending on data criticality;
- safekeeping in the computer room;
- safe transfer and storage of the additional backup to the offsite location;
- testing to ensure data integrity;
- proper backup filling and documentation on each media of the data context and the backup time;
- backup media recycling;

The second level is achieved through a complete and effective BCP and DRP for the Information Systems for which the following must apply:

1. It must be written in a simple and understandable language and officially communicated to all personnel. Privileged and confidential information (security codes, passwords etc.) included in the plan must be communicated to authorized personnel only.

2. A backup copy of the plan must be kept at a location safely distanced from the computer center.

Such a plan must include:

3. systems categorization according to their business importance. This list must, among other things, include each system's required recovery time and the expected level of functionality after the recovery;
4. a clear representation of the hierarchy and responsibilities of the personnel that participate in the plan along with the decision makers in every emergency action team;
5. procedures for defining the scale of disaster thus specifying which parts of the plans must be invoked in order to address the disaster at hand;
6. procedures for the plan invocation, the personnel notification and the emergency teams activation;
7. actions to be performed in specific emergency situations, including ways to ensure the safety of employees in cases of danger or destruction (for example fire, earthquake etc.);
8. alternative workplace/worksite arrangements, including the required infrastructure and relevant specifications;
9. procedures for the preparedness and activation of the alternative computer center;
10. the systems of the alternative center, their infrastructure along with the network topology and connections;
11. a list with the vendors under contracts, the services that they are obliged to provide as well as their response times in emergency situations mentioned in their service level agreements (SLAs);
12. procedures to ensure that the plans are managed, adjusted and updated with every change in the operational procedures of the FI;
13. the staff training procedures according to the responsibilities they have during the activation of the plan;
14. the testing procedures, according to which:
 - the frequency of tests must be defined (at least once a year)
 - clear goals must be specified beforehand either for the testing of certain subsystems or for full system testing. The full system test should cover all the critical operations as documented in the plan, the exclusive use of the disaster site, the infrastructure and backup copies

- the tests must be run under circumstances that simulate emergency situations
- the involvement of the Internal Audit function must be ensured
- after the completion of the tests, a report of results should be prepared
- any problems identified in the plans should be addressed by proper corrections and adjustments
- the results must be communicated to Management and the Audit Committee.

Finally it should:

15. ensure the effective operation of the alternative (disaster) computer centre that must be located in a safe distance from the main computer centre, so that it is not subject to the same risks as the main computer centre. The alternative computer centre should have the proper (redundant) equipment that will supply all the critical services within the predefined timeframes along with the systems procedure manuals and documentation. Additionally, all the alternative systems must operate effectively until the return of operations to the main computer centre.
16. ensure the physical security of the disaster site and a basic level of logical security during the plan operation.
17. take care of the insurance coverage of the FI against risks of information systems disruption .
18. in cases where the disaster site, the equipment or the services are provided by a vendor, the FI must:
 - ensure, through proper contractual arrangements, the effective continuity of operations in the event that the disaster strikes at the same time multiple organizations served by the same vendor
 - ensure that the vendor is kept informed of any changes in the FI's systems that might require extra adjustments/updates to the disaster recovery plans.

D. IT AUDIT

An effective audit function for the Information Systems should focus on the risks arising from their development, integration and operation, evaluate the adequacy of the control mechanisms and procedures and suggest, where necessary, the proper adjustments. The audit function must evaluate compatibility with the business strategy and the documented business standards, policies and procedures and compliance with the audit report findings. Finally a complete understanding should exist for the Information Systems operations and functions so that the audit function can deliver an informed opinion to the Audit Committee.

To this end, the Internal Audit Department should:

1. possess the know-how, the quality and quantity adequacy of staff, media and procedures for the execution of specific Information System audits. The staff knowledge and training should cover the current and future audit needs, in view of ongoing advances of Information Technology.
2. create and execute an audit plan based on an IT risk analysis and on previous audit report findings.
3. follow documented procedures for the audit design, organization and execution, audit report writing and structure and audit follow up. These procedures, the various questionnaires used during the specialized audits, along with the methodology for the IT risk analysis compose the formal documentation for the IT Audit operation.
4. monitor the matters related to the Financial Institution's Information Systems in order to have a comprehensive picture of existing or future risks. To facilitate a better understanding the IT Audit should supervise the operation of the IT systems through special audit accounts, participate in various project committees and use mechanisms and procedures for its immediate notification in cases of emergency or serious problems in the day to day operations of the FI.
5. use – depending upon circumstances – specialized audit software in order to perform a more effective security audit and ensure the integrity of data.
6. participate in the systems design phase in order to shape up the proper controls and the audit files and reports that will be produced to assist the work of the internal audit and also participate in the testing phase.
7. audit and evaluate the production procedures for the data sent to the FI Management and the Supervising Authorities in order to ensure the completeness and accuracy of the data.
8. ensure the immediate and complete notification of Bank of Greece's Supervision of Credit & Related Financial Institutions Department responsible organizational unit for incidents in the FI's Information Systems caused by serious problems and emergency circumstances (e.g. cases of, fraud, breach of security and non-availability of critical systems, activation of the disaster recovery plans).
9. audit and evaluate the adequacy and compliance with the procedures that govern the relationships of the FI (vendor selection, contract signing, quality of offered services) with suppliers and information services vendors based on the rules and guidelines mentioned in section A3.

10. oversee the information systems audit work at a Group level. To achieve this, along with an effective cooperation, the FI must maintain open communication channels with management and internal audit of its subsidiaries and branches abroad; evaluate the adequacy of the audit work through periodic reports or participation in the subsidiaries Audit Committees especially in those whose size and information systems complexity require such an approach; evaluate the adequacy and completeness of the special audits that take place from internal or external audit; engage in a wide range of special audits per case in order to cover audit needs that either cannot be catered efficiently from the units abroad Internal Audit or are deemed necessary based on a risk analysis.
11. study, evaluate and apply, where deemed appropriate, the international Information System Audit templates and procedures.

With regard to the audits conducted by external auditors, the Financial Institution should:

possess a policy that defines the scope role of the Information Systems external audit, as well as procedures for the evaluation of the offered services. This policy must address and document both cases, where external audit (i) acts in parallel with internal audit providing an additional specialized view or (ii) has a supplementary role, in order to cover specialized audit requirements that cannot be met internally.