Information System Risk Management System Checklist

Information system risk is the risk that an insurance company will incur losses because of down or malfunctioning computer systems or other computer system inadequacies, or because of improper use of computer systems.

Inspectors will verify and inspect the operational risk management systems of insurance companies using the“Risk Management Systems Checklists (Common Items)”, and this checklist. Should problems be identified in management systems and it be deemed necessary to engage in a deeper and more specific verification, inspectors shall refer to “Security Guidelines” and ”Explanation of Security Guidelines (edited by the Financial Institution Information Systems Center.

This checklist and manual apply to all insurance companies, including the foreign offices of Japanese insurance companies (foreign branch , foreign subsidiaries, and offices of the overseas workers, etc., though whether to include these offices in the inspection by this checklist and manual will be determined in light of applicable laws and ordinances, including applicable foreign-country laws and ordinances) and the Japan offices of foreign insurance companies.

[Notes on the use of this manual in inspections]

This manual is essentially a handbook to be used by inspectors in the inspection of insurance companies. It is expected that, as part of their efforts to ensure sound and proper operations and in accordance with the principle of self-responsibility, individual insurance companies will fully exercise their creativity and innovation to voluntarily create their own detailed manuals. These insurance company manuals should make note of the content of this manual and be adapted to the size and nature of the insurance company.

The check points in this manual represent standard to be used by inspectors in evaluating the risk management systems of insurance companies. They do not constitute direct statutory obligations to be achieved by insurance companies. Care must be taken that the manual is not adopted by rote and uniformly. If there may be cases in which the checklist description has not been fulfilled literally, by insurance company , in the light of ensuring the soundness and appropriateness of its operation only the time that the measures by insurance company are equivalent in their effects to the descriptions for the check point or are sufficient given the size and nature of the insurance company, these measures would not be deemed inappropriate.

Inspectors will therefore need to fully dialogue relevant points with insurance companies during on-site inspections.

In inspecting computer system risk management, inspectors will need to be fully aware of the importance and the nature of individual computer systems.

・Importance of computer systems refers to the size of the impact that a system has on customer transactions and judgement of business.

・Nature of computer systems refers to centralized main frame computer systems in computer centers, dispersal computer systems such as client/server configurations, stand-alone computer systems in user divisions, and the like, and the use of management methods that are appropriate to the system.

.Note: Explanation of check points

① Unless explicitly stated otherwise, items expressed in the question form such as “does the insurance company” or “is the insurance company” are minimum standards that are expected of all insurance companies. Inspectors, as they go through their checklists, need to fully verify the effectiveness of these items.

② Unless explicitly stated otherwise, items worded in the form of “it would be desirable that” constitute “best practice(sound practice)” for all insurance companies. Inspectors need only confirm these items.

Note: Distinction between “board of directors” and “board of directors, etc.”

① Items that are defined as roles of the “board of directors” are items for which the board of directors itself needs to determine all essential matters. This does not, however, preclude the board of directors from delegating consideration of draft documents to the management committee or similar bodies.

② The phrase “board of directors, etc.” includes the board of directors, the management committee, the management meeting, and similar bodies. Items that are defined as roles of the “board of directors, etc.” would ideally be determined by the board of directors itself, but may be delegated to the management committee, etc. provided that there has been a clear delegation of this authority from the board of directors, the management committee, etc. has kept minutes of its proceedings and other materials that would allow after-the-fact confirmation, and there are adequate internal checking by the measure the results are reported to the board of directors, or auditors are allowed to participate in the management committee, etc.

Note: Explanation of “business base”, “business bases”, “insurance sales”

① The phrase “business base” refers to organizations other than the head office that constitute business bases, such as branch offices, business headquarters, foreign branch offices, and foreign subsidiaries. The phrase “business bases” refers to organizations other than the head office that do not engage in sales activities, such as operating bases, service centers, and foreign liaison offices.

②The phrase “insurance sales” refers to insurance agency or insurance agent and does not include insurance broker.

Item	Risk Management System Check Point	Explanation of Risk Management Check Points	Remarks
I. Recognition of risk management etc. 1. Recognition of directors and role of board of directors	(1) Recognition of risk	(1) Does the board of directors establish risk management structure, with understanding that computer system risk introduce into business crisis when webbed computer network goes down sequentially, widely and seriously.	
	(2) Articulation of strategic goals based on management policies for the insurance company as a whole	(2) Does the board of directors articulate strategic goals? Do these strategic goals include strategic policies for computer systems that see computer systems as part of management strategy in light of IT innovation? Do strategic policies for computer systems specify: 1) system development priorities , 2) computerization promotion plans, 3) computer system investment plans and other relevant matters?	
	(3) Establishment of risk management policies	(3) Does the board of directors articulate basic policies for risk management? Do the basic policies for risk management include security policies (basic policies for the appropriate protection of the information of the organization) and outsourcing policies? Do security policies specify: 1) information to be protected, 2) reasons for protection, 3) locus of responsibility etc. for protection, and other relevant matters? Do outsourcing policies articulate, understanding that responsibility of accident on outsourced business for customer should be obligated insurance company. [reference] “Handbook for formulation of security policy in financial institutions” [FISK] Note: ”security policy” include not the recorded information in computer or medias but also the printed information in paper.	
	(4) Recognition and valuation of internet transaction risk	(4) Does insurance company understand the point of internet transaction risk that is the potential problem as non-counter, trouble, relationship of third party, etc? Does insurance company recognize and value the importance of these risk management.	
II. Establishment of appropriate risk management systems 1. Recognition and evaluation of risk	Identification of the locus and types of risk to be managed	1) Does the insurance company recognize and evaluate risks across the entire computer system, including evaluations of computer systems for different operational functions such as the accounting system, information system, external system, securities system, and international system? 2) If divisions other than the computer systems division build their own computer systems, does they recognize and evaluate the risks in these systems? 3) Does the insurance company recognize and evaluate the increasing diversity and degree of risk from the expansion of networks (the Internet, electronic mail) and the widespread use of personal computers?	
2. Division of responsibilities	Establishment of mutual checking systems	1) Do insurance companies divide responsibilities between computer systems development division and administration division in order to eliminate individual mistakes or malicious actions? However, if it is difficult for them to clearly separate the development and administration divisions because of staffing constraints, do they provide mutual checking, for example, in the form of regular rotations of staff between the development and administration divisions? Regardless of the organizations described above, does the internal audit division etc. provide checking functions for computer systems that by nature make it difficult to separate development and administration organizations, for example, end user computing (EUC)?	

Item	Risk Management System Check Point	Explanation of Risk Management Check Points	Remarks
		2) Does an internal audit division independent of the computer systems divisions perform regularly computer systems audit?	
III. Audit and correcting problems 1. Internal audits	(1) Organization of internal audit division	(1) 1) Do internal audit division that is independent of computer system division regularly system-audit? 2) Does the internal audit division have personnel versed in computer systems? Does insurance company establish structure as to able to corporate system-audit and other audit as necessary.	
	(2) Methods and content of internal audit performed by internal audit division	(2) 1) Do internal audit cover all operations that are related to computer (information) system risk? 2) Are computer systems divisions and divisions that establish their own computer systems audited by the head office in principle at least once per year? Does the internal audit division regularly audit computer system division and division owned self-computer-system in accordance with the level and sort of risk, gasping risk management status? 3) Are the procedures for use of computer equipment outside the computer systems divisions (for example, terminals and ATMs in branch offices) checked? 4) It is desirable that internal audit enable confirmation of auditing trails (journals and other records that trace processing content and the like) and provide evidence of the content of computer system operations.	
2. External audits	Use of external auditors	Do insurance companies regularly undergo external audits of computer system risk?	
IV. Planning and development structure 1. Planning and development structure	(1) Planning and development structure	(1) 1) Does the insurance company formulate planning and development rules to encourage the introduction of a highly reliable and efficient computer system? 2) It is desirable that the insurance company has a Computerization Committee or other company-wide screening organization. 3) Does the insurance company formulate medium- and long-term development plans? 4) Does the insurance company study the effects of investments in computer systems and report findings to the board of directors when necessary in light of the importance and nature of the system (and always for findings regarding investment effects for computer systems divisions as a whole)? 5) Does the insurance company have clear rules for studying and approving development proposals? 6) Are modifications etc. to functioning main systems subject to approval?	
	(2) Development management	(2) 1) Does the insurance company standardize development documentation and programming methods? 2) Does the insurance company assign responsibilities for individual development projects? Does the board of directors etc. check projects in light of the importance and nature of the computer system?	
	(3) Formulation of rules and manuals	(3) 1) Does the insurance company have rules and manuals for design, development and administration? 2) Does the insurance company review computer systems in light of operating? 3) It is desirable that the insurance company formulates standard requirements for design and development documents and create documents in conformity with these standards. 4) It is desirable that computer systems leave auditing trails (journals and other records that trace processing content and the like). 5) Are manuals and development documentation easily understood by technically competent third parties?	

Item	Risk Management System Check Point	Explanation of Risk Management Check Points	Remarks
	(4) Testing	(4) 1) Is testing appropriate and sufficient? 2) Does the insurance company have testing implementation organizations in place so as to prevent inadequate testing and reviews from causing problems that would have a prolonged influence on customers or serious malfunctions in the creation of risk management documents and other materials used in managerial decision-making? 3) Does the insurance company create testing plans? 4) It is desirable that user divisions participate in general tests. 5) Are acceptances made by executive personnel fully capable of understanding computer systems?	
	(5) Training	(5) 1) Does the insurance company train personnel in the operations for which systems are being developed, not just in development technology? 2) It is desirable that development personnel be versed in derivatives, electronic payments, electronic commerce, and other areas requiring a high degree of specialization, and also in technologies.	
	(6) Consignees management	(6) 1) Does the insurance company make confidentiality agreements when they consign computer systems development to consignees? 2) Does the insurance company restrict as necessary on the data accessible by temp-staff seconded from consignees?	
2. Expansion into new business	Expansion into new business	It is desirable that the insurance company gather and research information on new fields and new technologies, and study its position vis-à-vis management strategy.	
V. Establishment of structure 1. Management structure	(1) Security management structure	(1) 1) Does the insurance company assign security managers to appropriately manage security in accordance with established policies, standards, and procedures? Note: The following are examples of perspectives that might be used in security. a) Physical security ?Prevention measures of physical intrusion ?Security equipment ?Enhancement to computer operations environments ?Maintenance and check of equipment b) Logical security ?Mutual checking structure among and within development and administrative organizations ?Development management structure ?Prevention measures of electronic intrusion ?Program management ?Countermeasures on the time of system failure ? Evaluation and management of outside software packages at the time of introduction ?Operational security management etc. 2) Do security managers control the management structure for computer systems, data, and networks?	

Item	Risk Management System Check Point	Explanation of Risk Management Check Points	Remarks
	(2) Computer system management structure	(2) 1) Does the insurance company have computer system management procedures in place to ensure safe and smooth operation of computer systems and prevent unauthorized access? Does it assign computer system managers to provide appropriate management?	
	(3) Data management structure	(3) 1) Does the insurance company assign data managers to ensure the confidentiality, completeness, and utility of data? 2) Does the insurance company provide for safe and smooth utilization of data by formulating rules and manuals covering data management procedures and use authorization procedures etc. and ensuring that relevant employees are thoroughly familiar with these rules and manuals? 3) Does the insurance company have appropriate and adequate structure to protect data, prevent unauthorized use of data, and prevent the introduction of unauthorized programs? (Reference) "Guidelines on the Protection of Personal Data for Financial Institutions" (revised edition) (edited by the Financial Institution Information Systems Center)	
	(4) Network management structure	(4) 1) Does the insurance company assign network managers to appropriately manage network operations and control and monitor access? 2) Does the insurance company provide for safe and smooth network operations by formulating rules and manuals covering network management procedures and use authorization procedures and ensuring that relevant employees are thoroughly familiar with these rules and manuals? 3) Does the insurance company provide for alternate methods in going down networks?	
	(5) Management structure of insurance sales with inter-net	(5) 1) Does insurance company establish structure receive the complaint and reference? 2))Does insurance company establish structure to support operation, when computer system has trouble on customer or insurance company side? Does insurance company clarify the responsibility in system-down? 3) Does insurance company take measure to prevent from mis-recognition of servicer in web-linkage? 4) Does insurance company disclose the information of financial status and business and internet transaction service in homepage or so? 5) Does insurance company establish structure as to identify in order to prevent from money laundering? 6Does insurance company establish structure to prevent from divulging the customer information and falsification of data by evaded of outsider or insider. 7) Does the insurance company record the transaction informations of customer for a period as necessary, being aware that the internet transaction is non-counter?	

Item	Risk Management System Check Point	Explanation of Risk Management Check Points	Remarks
2. Computer system administration structure	(1) Clarification of work responsibilities	(1) 1) Does the insurance company clearly separate responsibilities for data reception, operations, work results verification, and data program storage? 2) Does the insurance company ban operators from accessing data and program outside of their work responsibility?	
	(2) Computer systems operation management	(2) 1) Does the insurance company engage in routine work based on work schedules, instruction lists? 2) Does the insurance company engage in operations based on approved work schedules and instructions? 3) Does the insurance company record all operations and have managers check them based on predefined checklists? 4) It is desirable that the insurance company enable important operations to be performed by multiple persons or, wherever possible, automate their performance. 5) Does the insurance company provide for report outputs and obtain and keep work records so that managers are able to check operations processing results? 6) Does the insurance company ban developers in principle from accessing operations? Does the insurance company provide for identification of developers and after-the-fact checking of access by operations managers in the event that development personnel must access operations, for example, in order to remedy failures?	
	(3) Trouble management	(3) 1) Does the insurance company require records to be filled out and as necessary reports to be issued to the head office in troubles? 2) Does the insurance company regularly analyze the contents of trouble and take necessary countermeasures? 3) In the important troubles that would have a serious influence on business, do divisions work speedily in coordination with the head office to find solutions and do they report to the board of directors?	
	(4) Protection of customers data	(4) 1) Does the insurance company in principle prohibit the disclosure of customers data to third parties except as permitted by law or agreed to by the customers? Does the insurance company provide for appropriate management of customers data handling by assigning managerial responsibilities and formulating management methods and handling methods? 2) Does the insurance company have appropriate safety measures to counteract the risk of unauthorized access to customers data, or the loss, damage, falsification, or disclosure of customers data? 3) Does insurance company appropriately manage the important information other than customer information, determinating manager and management method? [Reference] “Guideline of protecting personal information in financial institutions”[FISK]	
	(5) Prevention of unlawful access	(5) 1) Does the insurance company have systems to prevent unlawful access by confirming the identity of the person or terminal accessing systems as appropriate for the nature of the operation and the connection method? 2) Does the insurance company obtain computer system operation records as an auditing trail to manage unlawful access and enable after-the-fact auditing and regular checking? 3) Does insurance company establish the management method of access authorization to using computer, data and file as importance?	

Item	Risk Management System Check Point	Explanation of Risk Management Check Points	Remarks
	(6) Computer viruses etc.	(6) Does the insurance company have structure in place to prevent the introduction of computer viruses and other unlawful programs? Does it have structure in place to quickly discover and eliminate these programs in the event of occurrence? ? Computer virus infection ? Records of programs that have not gone through standard procedures ? Intentional interpolation of authorized programs	
VI. Outsourced business management	(1) Plan and implementation of outsourcing	(1) Does the insurance company determine the extent of outsourcing and formulate the concrete measures	
	(2) Risk management structure of outsourced business	(2) 1) Does the insurance company assign the manager who appropriately manage outsourced computer system and/or business? 2) Does the insurance company establish structure to manage the risk (include structure of risk recognition and valuation, corrections, and so on) fully with contracts? 3) Does the insurance company make confidentiality agreements on outsourcing computer systems development to outsourcee? 4) Does the insurance company restrict on the data accessible by temp-staff seconded from outsourcee? 5) Does the insurance company assess the outsourced business and outsourcee regularly? It is desirable that outsourced business is assessed by the third party institution as business contents.	
	(3) Correction of problems	(3) Does the insurance company correct the gasped problem with outsourcee?	
VII. Security, disaster prevention back-ups, and prevention of unlawful access	(1) Security	(1) 1) Does the insurance company have an anti-crime organization and manager in order to prevent criminal activities? 2) Does the insurance company engage in appropriate and adequate management designed to prevent actions that would threaten the safety of computer systems, for example, management of entry and exit from work areas, management of important keys etc.?	
	(2) Computer crimes and accidents	(2) Does the insurance company have organizations that are fully aware of computer crime (penetration of viruses and unauthorized programs, destruction of CD/ATM equipment and theft of cash, card fraud, stole by outsider, divulging of the information by insider, trouble of hard and soft etc.) and computer accidents (hardware and software failures, operational mistakes, telecommunication failures, power outages, external computer failures etc.)? Does it have systems for after-the-fact checking as internal audit or self-checking?	
	(3) Disaster prevention	(3) 1) Does the insurance company have a disaster-prevention organization and manager to reduce damage and carry on work in the event of disaster? 2) Is the disaster-prevention organization in line with business organizations, and are there clear separate roles for individual operations? 3) Does the insurance company have measures to combat damage from fire, earthquake, and flooding? 4) Does the insurance company have predetermined evacuation points for important data etc?	

Item	Risk Management System Check Point	Explanation of Risk Management Check Points	Remarks
	(4) Back-ups	(4) 1) Does the insurance company obtain back-ups to enable response in the event of damage or failure of important data files and programs? Does it formulate clear management methods therefore?	
	(5) Formulation of contingency plans	(5) 1) Does the insurance company formulate contingency plans to prepare for disasters and other events that would prevent computer systems from functioning in a normal manner? 2) Does the insurance company seek approval from the board of directors in the formulation and any important reviews of its contingency plans? (Does it then seek approval of the board of directors etc. for other, less-important reviews?) 3) Does the insurance company refer its contingency plans to "Contingency Plan Procedures for Financial Institutions" and "Contingency Plan Formulation Manual for Financial Institutions" (edited by the Financial Institution Information Systems Center)? 4) Does the insurance company envision causes from within and outside the company in the formulation of its contingency plans, not just disasters and other emergencies? 5) Does the insurance company analyze the impact on the payments system and the damage to customers in the formulation of contingency plans? 6) Does the insurance company train on its contingency plan regularly?	