FISC Security Guidelines on Computer Systems for Banking and Related Financial Institutions

Amazon Web Services Response, June 2012

Major Item	Medium Item	Item No	Minor Item	AWS Response
Buildings	**Environment**	F1	Avoid setting up compute center in a place subject to disasters or failures	AWS data centers are state of the art, utilizing innovative architectural and engineering approaches and incorporates physical protection against environmental risks. Refer to the "Amazon Web Services Overview of Security Processes" whitepaper available at http://aws.amazon.com/security for additional information. In addition, ISO 27001 standard, Annex A domain 9.1 and AWS SOC 1 Type 2 report provides further detail. AWS has been validated and certified by an independent auditor to confirm alignment with ISO 27001 certification standard.
	Surroundings	F2	Identify the potential of being subject to disasters and failures due to changes of site environment and develop proper preventive measures	AWS datacenters are housed in nondescript facilities. Physical security controls include but are not limited to perimeter controls such as fencing, walls, security staff, video surveillance, intrusion detection systems and other electronic means. The AWS SOC 1 Type 2 report provides additional details on the specific control activities executed by AWS. Refer to ISO 27001 standard, Annex A, domain 9.1 for further information. AWS has been validated and certified by an independent auditor to confirm alignment with ISO 27001 certification standard.
		F3	Secure proper routes on the premises	
		F4	Provide adequate clearance against adjacent structures	
		F5	Install walls or fences, and equipment to prevent burglary	
		F6	Do not install a signboard, etc. outside	
		F7	Protect the buildings with proper lightning protection facility	
		F8	Make the building available only for computer 'system-related operations, or establish an' independent zone for computer system-related operations in a building	
		F9	Take measures to protect communication and power lines within a site from breakage and spread of fire	
	Structures	F10	Ensure that the buildings are fire-resistant	AWS data centers incorporate physical protection against environmental risks. AWS's physical protection against environmental risks has been validated by an independent auditor and has been certified as being in alignment with ISO 27002 best practices. Refer to ISO 27001 standard, Annex A domain 9.1 and the AWS SOC 1 Type 2 report for additional information.
		F11	Ensure the safety of building structure	
		F12	Ensure that building exterior walls, roofs, and other structural members are water-resistant	
		F13	Ensure adequate strength of exterior walls	
h	**Openings**	F14	Ensure that the windows are provided with fireproofing capabilities	Physical security controls include but are not limited to perimeter controls such as fencing, walls, security staff, video surveillance, intrusion detection systems and other electronic means. The AWS SOC 1 Type 2 report provides additional details on the specific control activities executed by AWS. Refer to ISO 27001 standard, Annex A, domain 9.1 for further information. AWS has been validated and certified by an independent auditor to confirm alignment with ISO 27001 certification standard.
		F15	Ensure that proper crime-prevention systems are installed	
		F16	Designate only one entrance as a usual entrance, and install access control equipment and security equipment	

Major Item	Medium Item	Item No	Minor Item	AWS Response
		F17	Install emergency exits	
		F18	Provide proper waterproof measures	
		F19	Install entrance doors with sufficient strength and add locks .	
	Interior finish	F20	Use building interior items made of non-combustible materials and having sufficient flame retardation efficiency	AWS data centers incorporate physical protection against environmental risks. AWS's physical protection against environmental risks has been validated by an independent auditor and has been certified as being in alignment with ISO 27002 best practices. Refer to ISO 27001 standard, Annex A domain 9.1 and the AWS SOC 1 Type 2 report for additional information.
		F21	Make proper provisions for prevention of falling or broken interior items in the event of earthquake	
Computer Room and Data Storage Room	**Location**	F22	Install the computer room and data storage room in proper locators that are less susceptible to disasters	AWS datacenters are housed in nondescript facilities. AWS data centers incorporate physical protection against environmental risks. Refer to the "Amazon Web Services Overview of Security Processes" whitepaper available at http://aws.amazon.com/security for additional information. In addition, ISO 27001 standard, Annex A domain 9.1 and AWS SOC 1 Type 2 report provides further detail. AWS has been validated and certified by an independent auditor to confirm alignment with ISO 27001 certification standard.
		F23	Install the computer room and data storage room in proper locations accessible from the outside	
		F24	Do not install any signs indicating the names of rooms	
		F25	Keep the necessary space .	
		F26	A computer room and a data storage room must be separate-dedicated rooms	
	Openings	F27	Designate only one entrance as a usually entrance, and provide it with a preparatory room	AWS Data Centers are housed in nondescript facilities. Physical security controls include but are not limited to perimeter controls such as fencing, walls, security staff, video surveillance, intrusion detection systems and other electronic means. The AWS SOC 1 Type 2 report provides additional details on the specific control activities executed by AWS. Refer to ISO 27001 standard, Annex A, domain 9.1 for further information. AWS has been validated and certified by an independent auditor to confirm alignment with ISO 27001 certification standard.
		F28	Install entrance doors of sufficient strength and add locks	
		F29	Apply fireproofing and water proofing to windows, and take measures to prevent them being broken and equipment in the room from being seen from the outside	
		F30	Install emergency exits, evacuation apparatus, and guide lights	
	Structure and interior finish	F31	Define the computer room and data storage room as independent fire retarding	AWS data centers incorporate physical protection against environmental risks. Refer to the "Amazon Web Services Overview of Security Processes" whitepaper available at http://aws.amazon.com/security for additional information. In addition, ISO 27001 standard, Annex A domain 9.1 and AWS SOC 1 Type 2 report provides further detail. AWS has been validated and certified by an independent auditor to confirm alignment with ISO 27001 certification standard.
		F32	Provide proper water leakage-prevention measures	
		F33	Provide proper protection against static electricity	
		F34	Use non.-combustible and flame-proof materials for interior items	

Major Item	Medium Item	Item No	Minor Item	AWS Response
		F35	Make proper provisions for prevention of possible falling or damage of interior items in the event of earthquake	
		F36	A free-access floor must be constructed as earthquake resistant, so that it is not damaged in the case of earthquakes	
	Facilities	F37	Install automatic fire alarm systems	AWS data centers incorporate physical protection against environmental and security risks. This includes but is not limited to fire detection and suppression, climate control to maintain atmostphereic conditions at optimal levels and physical security controls. Refer to the "Amazon Web Services Overview of Security Processes" whitepaper available at http://aws.amazon.com/security for additional information. In addition, ISO 27001 standard, Annex A domain 9.1 and AWS SOC 1 Type 2 report provides further detail. AWS has been validated and certified by an independent auditor to confirm alignment with ISO 27001 certification standard.
		F38	Install proper communications systems in preparation for any emergency	
		F39	Install fire extinguishing systems	
		F40	Render the cables flame retardant and resistant to fire spreading	
		F41	Install proper smoke exhaustion equipment	
		F42	Install proper emergency lighting equipment and portable lighting fixtures	
		F43	Do not install any equipment that uses water	
		F44	Install seismic detectors	
		F45	Install access control and security facilities at entrances	
		F46	Install automatic temperature and humidity recorders or alarm systems for any exceptional temperature/humidity	
		F47	Make proper provisions against possible damage by rats	
	Compute equipment,fixtures,and furnishings	F48	Ensure that fixtures and furnishings are incombustible	AWS data centers incorporate physical protection and precautions against local environmental risks including sesimic events. Refer to the "Amazon Web Services Overview of Security Processes" whitepaper available at http://aws.amazon.com/security for additional information.
		F49	Provide proper protection against static electricity	
		F50	Take proper precautions against possible earthquake	
		F51	Carriages, carts, and other. equipment should be fixtures, and provided with proper locking devices	
Power Supply Rooms and Air-Conditioner Rooms		F52	Install the power supply room and air-conditioner room in a place less susceptible to disaster	AWS data centers incorporate physical protection against environmental risks. This includes but is not limited to fire detection and suppression, climate control to maintain atmostphereic conditions at optimal levels and power systems designed to be fully redundant. Physical security controls include but are not limited to perimeter controls such as fencing, walls, security staff, video surveillance, intrusion detection systems and other electronic means. Refer to the "Amazon Web Services Overview of Security Processes" whitepaper available at http://aws.amazon.com/security for additional information. In addition, ISO 27001 standard, Annex A domain 9.1 and AWS SOC 1 Type 2 report provides further detail. AWS has been validated and certified by an independent auditor to confirm alignment with ISO 27001 certification standard.
		F53	Provide adequate space for inspection and maintenance	
		F54	Use independent, dedicated rooms for power supply room and air-conditioner room	
		F55	Do not install any windows, but install locked doors	
		F56	Adopt fire-resistant structures	
		F57	Install automatic fire alarm systems	
		F58	Install gas-based fire extinguishing systems	
		F59	Take precautions for preventing water leakage from air-conditioning facilities	

Major Item	Medium Item	Item No	Minor Item	AWS Response
		F60	Take proper precautions against fire spreading from cables and ducts	
Power supply facilities		F61	Allow an adequate margin for capacity of the power supply facilities	The data center electrical power systems are designed to be fully redundant and maintainable without impact to operations, 24 hours a day and seven days a week. Uninterruptible Power Supply (UPS) units provide back-up power in the event of an electrical failure for critical and essential loads in the facility. Data Centers use generators to provide back-up power for the entire facility. Refer to the "Amazon Web Services Overview of Security Processes" whitepaper available at http://aws.amazon.com/security for additional information. In addition, ISO 27001 standard, Annex A domain 9.1 and AWS SOC 1 Type 2 report provides further detail. AWS has been validated and certified by an independent auditor to confirm alignment with ISO 27001 certification standard.
		F62	Use multiple lead-in lines to draw in the power source	
		F63	Install a proper power supply facilities to supply electric power of high quality	
		F64	Install a private power generation facility and a battery facility	
		F65	Provide the power supply facilities with lightning protection facilities	
		F66	Provide the power supply facilities with proper provisions against earthquake	
		F67	Use dedicated equipment and lines to draw in the power source a distribution board to computer devices	
		F68	Avoid combined use with any device involving significantly varying loads	
		F69	Provide the computer systems with dedicated grounding	
		F70	Make proper provisions against damage to each device due to over-current or leakage of electricity	
		F71	Install proper emergency power generators for disaster control and crime prevention systems	
Air-conditioning facilities		F72	Ensure that air-conditioning facilities have an adequate margin of capacity	AWS data centers are developed to incorporate physical protection against environmental and security risks. Climate control is required to maintain a constant temperature for servers and other hardware which prevents overheating and reduces the posiblity of service outages. Data Centers are conditioned to maintain atmostphirc conditions at optimal levels. Personnel and systems monitor and control temperature and humidity at appropriate levels. Refer to ISO 27001 standard, Annex A domain 9.1 and AWS SOC 1 Type 2 report provides further detail. AWS has been validated and certified by an independent auditor to confirm alignment with ISO 27001 certification standard.
		F73	The air-conditioning facilities should have proper provisions for stable air conditioning	
		F74	Use the air-conditioning facilities dedicated for the computer room	
		F75	Install a backup air-conditioning facilities	
		F76	Provide the automatic control units the emergency alarms for the air-conditioning facilities	
		F77	Take measures against intrusion and destruction of air-conditioning facilities	
		F78	Provide the air-conditioning facilities with proper protection against earthquake	
		F79	Insulation materials and air supply and exhaust openings for air-conditioning facilities should be made from noncombustible materials	

Major Item	Medium Item	Item No	Minor Item	AWS Response
Monitor and Control System		F80	Install the monitor and control system	AWS monitors electrical, mechanical, physical security and life support systems and equipment so tha tany issues are immediately identified. Refer to the "Amazon Web Services Overview of Security Processes" whitepaper available at
		F81	Install the central control and monitoring station	
(VII) Line-Related System		F82	Protect the line-related systems with proper locks	*Physical security controls include but are not limited to perimeter controls such as fencing, walls, security staff, video surveillance, intrusion detection systems and other electronic means. This includes appropriate protection for network cables.* *The AWS SOC 1 Type 2 report provides additional details on the specific control activities executed by AWS.* *Refer to ISO 27001 standard, Annex A, domain 9.1 for further information. AWS has been validated and certified by an independent auditor to confirm alignment with ISO 27001 certification standard.*
		F83	Do not install any label to the line-related systems referring to indicate the installed location	
		F83-1	Install the lines in the dedicated cabling space	
Security management definition of responsibility	**Security management and definition of responsibility**	O1	Documentation should be prepared with concrete definitions of security management methods	In alignment with ISO 27001 standards, policies and procedures have been established through AWS Information Security framework. The control environment at Amazon begins at the highest level of the Company. Executive and senior leadership play important roles in establishing the Company's tone and core values. Refer to AWS Risk and Compliance Whitepaper for additional details - available at http://aws.amazon.com/security.
		O2	Documentation that defines security management methods in concrete terms should be evaluated and revised	
		O3	Establish a security management system	
		O4	Establish a system management system	
		O5	Establish a data management system	
		O6	Establish a network management system	
	Establish of organization	O7	Establish and maintain an organization for disaster prevention	AWS' Compliance and Security teams have established an information security framework and policies based on the Control Objectives for Information and related Technology (COBIT) framework. The AWS security framework integrates the ISO 27002 best practices and the PCI Data Security Standard. Refer to AWS Risk and Compliance Whitepaper for additional details - available at http://aws.amazon.com/security.
		O8	Establish a proper crime prevention organization	
		O9	Establish operational organizations	
	Formulate regulations	O10	Establish various regulations	AWS maintains contacts with industry bodies, risk and compliance organizations, local authorities and regulatory bodies as required by the ISO 27001 standard.
	Confirm security observance status	O10-1	Confirm the status of security observance	AWS obtains certain industry certifications and independent third party attestations and provides certain certifications, reports and other relevant documentation directly to AWS customers under NDA.
Physical access control	**Physical access control(building and rooms)**	O11	Establish proper authorization and key control system	Physical access is strictly controlled both at the perimeter and at building ingress points by professional security staff utilizing video surveillance, intrusion detection systems, and other electronic means. Authorized staff must pass two-factor authentication a minimum of two times to access datacenter floors. Refer to AWS Overview of
		O12	Execute physical access control	

Major Item	Medium Item	Item No	Minor Item	AWS Response
		O13	Execute room access control	Security Processes Whitepaper for further information available at http://aws.amazon.com/security. In addition, the AWS SOC 1 type 2 report provides additional details on the specific control activities executed by AWS.
Operational management	**Documentation**	O14	Document and maintain manuals for operation in normal times	Information System Documentation is made available internal to AWS personnel through the use of Amazon's Intranet site. Refer to AWS Overview of Security Processes Whitepaper for additional details - available at http://aws.amazon.com/security. AWS Business Continuity Policies and Plans have been developed and tested in alignment with ISO 27001 standards. Refer to ISO 27001 standard, annex A domain 14.1 and AWS SOC 1 report for further details on AWS and business continuity.
		O15	Prepare manuals used in case of a failure or disaster	
	Access authority management	O16	Definition of access authority to resources and systems	In alignment with ISO 27001 standards, AWS has established formal policies, procedures to delineate the minimum standards for logical access to AWS resources. AWS SOC 1 Type 2 report outlines the controls in place to manage access provisioning to AWS resources. Refer to AWS Overview of Security Processes whitepaper for additional details - available at http://aws.amazon.com/security.
		O17	Takes proper precautions not to make passwords known to anyone other than respective users	
		O18	Define the procedures for authorizing access to various resources and systems and reviewing the access authorization	
	Management of operations	O19	Verify operator qualifications	AWS has implemented various methods of internal communication to help employees understand their individual roles and responsibilities. These methods include orientation and training programs for newly hired employees, regular management meetings fo updates on business performance and electronic means such as video conferencing, electronic mail messages and the posting of information via the Amazon Intranet. Refer to the "Amazon Web Services Overview of Security Processes" whitepaper available at http://aws.amazon.com/security for additional information.
		O20	Define the procedures for assignment and approval of operations	
		O21	Establish and maintain an organization for system operations	
		O22	Make a record for checking of operations	
		O23	Manage operations in a client-server system	
	Input management	O24	Manage data input	AWS customers retain control and ownership of their data and it is the customers responsibility for managing data input.
	Data file management	O25	Establish transfer and management methods	AWS customers retain control and ownership of their data and associated procedures for managing transfer and revision control of data files.
		O26	Define the procedures for revision control of data files	

Major Item	Medium Item	Item No	Minor Item	AWS Response
		O27	Maintain backup copies	AWS provides customers the flexibility to place instances and store data within multiple geographic regions as well as across multiple Availability Zones within each region. Customers should architect their AWS usage to take advantage of multiple Regions and Availability Zones as distributing applications across multiple Availability Zones provides the ability to remain resilient in the face of most failure modes including natural disasters or system failures.
	Program file management	O28	Establish and maintain procedures for control of program files	AWS customers retain control and ownership of their data and associated program files. AWS provides customers the flexibility to place instances and store data within multiple geographic regions as
		O29	Maintain backup copies	
	Measures against computer viruses	O30	Take measures against computer viruses	AWS's program, processes and procedures to managing antivirus / malicious software is in alignment with ISO 27001 standards. Refer to AWS SOC 1 Type 2 report provides further details. In addition, refer to ISO 27001 standard, Annex A, domain 10.4 for additional details. AWS has been validated and certified by an independent auditor to confirm alignment with ISO 27001 certification standard.
	Network setting information management	O31	Implement configuration management	Emergency, non-routine and other configuration changes to existing AWS infrastructure are authorized, logged, tested, approved and documented in accordance with industry norms for similar systems.
		O32	Maintain backup copies of configuration	
	Document management	O33	Storage management defined	AWS customers retain control and ownership of their data and associated procedures for storage management of data.
		O34	Maintain backup copies	
	Forms management	O35	Establish a method for managing unused important forms	AWS customers retain control and ownership of their data and associated forms.
		O36	Establish and maintain the procedures for handling of important printed forms	
	Output management	O37	Take measures for prevention from unauthorized action and the protection of secrecy in making and handling output information	AWS customers retain control and ownership of their data and associated measures for management of handling output information.
	Transaction management	O38	Define operational authority for each transaction	AWS customers retain control and ownership of their data and associated measures of transaction management.
		O39	Properly control the operator cards	
		O40	Keep a log of operations for transactions and inspect the log	
		O41	Establish for reception system of reports from customers, and implement the management of troubled accounts	
		O42	State the loss that user ma suffer, and his or her responsibility accompanying the t	

Major Item	Medium Item	Item No	Minor Item	AWS Response
	Cryptographic key management	O43	Operational management methods should be defined for the use of cryptographic keys	AWS Customers manage their own encryption unless they are utilizing AWS server side encryption service. AWS allows customers to use their own encryption mechanisms for nearly all the services, including S3, EBS, SimpleDB and EC2. VPC sessions are also encrypted. Amazon S3 also offers Server Side Encryption as an option for customers. Customers may also use third-party encryption technologies. AWS key management procedures are in alignment with ISO 27001 standard. Refer to ISO 27001 standard, Annex A, domain 15.1 for additional details. AWS has been validated and certified by an independent auditor to confirm alignment with ISO 27001 certification standard. Refer to AWS Overview of Security Processes Whitepaper for additional details - available at http://aws.amazon.com/security.
	Strict ID confirmation	O44	Implement personal identification	AWS customers retain control and ownership of their data and associated controls for managing financial transactions
		O44-1	Ensure the financial transactions by duly authorized customers in the cash transactions through CD/ATM, an other automated machines.	
	Management of CD/ATM, and unmanned branch	O45	Establish operational management methods and take appropriate precautions against possible illicit withdrawals	AWS customers retain control and ownership of their data and associated controls for managing financial transactions
		O46	Establish and maintain proper monitoring system	
		O47	Definition of the security system	
		O48	Establish and maintain proper preparedness for any failure of disaster	
		O49	Document and maintain required manual	
	Management of handheld terminals	O50	Establish and maintain proper procedures for operation and management	AWS customers retain control and ownership of their data and associated controls for managing their handheld terminals.
	Management of cards	O51	Establish a method for managing cards	AWS customers retain control and ownership of their data and associated controls for managing cards.
		O51-1	Raise customer's awareness about crimes	
		O52	Define the proceedures for monitoring transactions by using card in any designated accounts	
	Protection of customer data	O53	Take measures for protection of customer data	AWS customers retain control and ownership of their data and associated controls for managing biometrics information.
		O53-1	Implement the security control measures for biometrics information handled in the process of biometric authentication	
	Resource management	O54	Check individual resources for the capability and usage	Customers retain control of their own guest operating systems, software and applications and are responsible for managing individual resources for the capability and usage.
	External connection management	O55	Define the connection of contract for external connection	Customers retain control of their own guest operating systems, software and applications and are responsible for operational management methods for external connections.

Major Item	Medium Item	Item No	Minor Item	AWS Response
		O56	Establish operational managament methods for external connections	
	Devices management	O57	Definition of managament method	Customers retain control of their own guest operating systems, software and applications and are responsible for defining procedures to manage their devices.
		O58	Take measures to protect network-related devices	
		O59	Define the procedures for maintaining the devices	
	Monitoring operations	O60	Establish proper monitoring system	Customers retain control of their own guest operating systems, software and applications and are responsible for defining monitoring procedures. AWS Cloudwatch provides monitoring for AWS cloud resources and the applications customers run on AWS. Refer to aws.amazon.com/cloudwatch for additional details. AWS also publishes our most up-to-the-minute information on service availability on the Service Health Dashboard. Refer to status.aws.amazon.com.
	Computer room and data storage room management	O61	Operations conducted after entry into the room should be managaed	Physical access is strictly controlled both at the perimeter and at building ingress points. Authorized staff must pass two-factor authentication a minimum of two times to access datacenter floors. Every employee is provided with the Company's Code of Business Conduct and Ethics and completes periodic Information Security training which requires an acknowledgement to complete. Compliance audits are periodically performed to validate that employees understand and follow the established policies
	Measures for handling Failures and disasters	O62	Define the procedures for comminicating with those who are responsible for control of failures and disasters	AWS provides customers the flexibility to place instances and store data within multiple geographic regions as well as across multiple Availability Zones within each region. Customers should architect their AWS usage to take advantage of multiple Regions and Availability Zones. Refer to AWS Overview of Security Processes whitepaper for additional details - available at http://aws.amazon.com/security
		O63	Establish definite measures against failures and disasters	
		O64	Identify and analyze possible causes of any failure	
	Formulate contingency plans	O65	Formulation of a contingency plans	AWS Business Continuity Policies and Plans have been developed and tested in alignment with ISO 27001 standards. Refer to ISO 27001 standard, annex A domain 14.1 and AWS SOC 1 report for further details on AWS and business continuity.

Major Item	Medium Item	Item No	Minor Item	AWS Response
System Development and Modification	**Hardware and software managament**	O66	Hardware and sofware management should be performed	In alignment with ISO 27001 standards, AWS Hardware assets are assigned an owner, tracked and monitored by the AWS personnel with AWS proprietary inventory management tools. Refer to ISO 27001 standard, Annex A, domain 7.1 for additional details. AWS has been validated and certified by an independent auditor to confirm alignment with ISO 27001 certification standard. AWS incorporates standards of quality as part of the system development lifecycle (SDLC) processes which are in alignment with ISO 27001 standard. Refer to ISO 27001 standard, Annex A, domain 10.1 for additional details. AWS has been validated and certified by an independent auditor to confirm alignment with ISO 27001 certification standard.
	System development and modification management	O67	Establish definite development and modification procedures	AWS Customers retain the ability and the responsibility to create and maintain production and test environments. AWS website provides guidance on creating an environment utilizing the AWS services - http://aws.amazon.com/documentation/.
		O68	Establish proper test environments	
		O69	Define the procedures for transition to production	
	Document managament	O70	Establish the procedures for preparing system documents	In alignment with ISO 27001 standards, AWS maintains system baselines for critical components. Refer to ISO 27001 standard, Annex A, domain 12.1 and 15.2 for additional details. AWS has been validated and certified by an independent auditor to confirm alignment with ISO 27001 certification standard. Customers are responsible for the development, content, operation, maintenance, and use of their documents and use of storage.
		O71	Define the procedures for proper storage managament	
	Package installation	O72	Establish a proper evaluation organization	AWS Customers retain control of their own guest operating systems, software and applications and are responsible for managing packages.
		O73	Establish and maintain proper operation and managemen organization for packages	
	Disposal of systems	O74	Establish a disposal plan and a procedure for systems	In alignment with ISO 27001 standards, when a storage device has reached the end of its useful life, AWS procedures include a decommissioning process that is designed to prevent customer data from being exposed to unauthorized individuals. AWS uses the techniques detailed in DoD 5220.22-M (“National Industrial Security Program Operating Manual “) or NIST 800-88 (“Guidelines for Media Sanitization”) to destroy data as part of the decommissioning process. If a hardware device is unable to be decommissioned using these procedures, the device will be degaussed or physically destroyed in accordance with industry-standard practices. Refer to ISO 27001 standard, Annex A, domain 9.2 for additional details. AWS has been validated and certified by an independent auditor to confirm alignment with ISO 27001 certification standard.
		O75	Take measures to prevent leakage of information	
Facility management	**Maintenace and management**	O76	Establish a method for managing facilities	AWS monitors electrical, mechanical, physical security and life support systems and equipment so that any

Major Item	Medium Item	Item No	Minor Item	AWS Response
		O77	Establish and maintain procedures for maintenance of facilities	issues are immediately identified. Preventative maintenance is performed to maintain the continued operability of equipment Refer to the "Amazon Web Services Overview of Security Processes" whitepaper available at http://aws.amazon.com/
	Resource management	O78	Identify available capalibities and actual conditions of use	Resource utilization is monitored by AWS as necessary to effectively manage the availability of the service.
	Monitoring	O79	Establish and maintain a proper monitoring organization	AWS monitors electrical, mechanical, physical security and life support systems and equipment so that any issues are immediately identified. AWS Cloudwatch provides monitoring for AWS cloud resources and the applications customers run on AWS. Refer to aws.amazon.com/cloudwatch for additional details. AWS also publishes our most up-to-the-minute information on service availability on the Service Health Dashboard. Refer to status.aws.amazon.com.
Education and Training	**Education and Training**	O80	Carry out security training	AWS has implemented various methods of internal communication to help employees understand their individual roles and responsibilities. These methods include orientation and training programs for newly hired employees, regular management meetings fo updates on business performance and electronic means such as video conferencing, electronic mail messages and the posting of information via the Amazon Intranet. Refer to the "Amazon Web Services Overview of Security Processes" whitepaper available at http://aws.amazon.com/security for additional information.
		O81	Carry out education to improve skills of personnel	
		O82	Provide proper education and training for mastering system operation	
		O83	Provide proper education and training for failures and disasters	
		O84	implement disaster prevention an crime prevention training	
Staff management	**Staff management**	O85	Appropriately perform personal managament	Every employee is provided with the Company's Code of Business Conduct and Ethics and completes periodic Information Security training which requires an acknowledgement to complete. Compliance audits are periodically performed to validate that employees understand and follow the established policies. Refer to AWS Overview of Security Processes Whitepaper for additional details - available at http://aws.amazon.com/security.
		O86	Implement proper health care for employees	
External Outsourcee Management	**External outsourcee management**	O87	Before outsourcing of computer systems development and operation,define the objectives and extent of outsourcing	AWS Customers retain the ability and the responsibility to manage external outsource management
		O87-1	Establish a outsourcee selection rule and contracting procedures	

Major Item	Medium Item	Item No	Minor Item	AWS Response
		O88	Conclude proper contracts for outsourcing, including the security control items	
	External outsourcee business managament	O89	Strict observance of rules by external outsourcee's staff sould be assured, and the state of their observance should be managed and confirmed	AWS Customers retain the ability and the responsibility to manage external outsource management
		O90	Establish an operational organaization for externally outsourced operations, and manage and confirm the work done	
		O90-1	Manage risk for network that connect each banks	
System Auditing	**System auditing**	O91	Establish system auditing structures	AWS obtains certain industry certifications and independent third party attestations and provides certain certifications, reports and other relevant documentation directly to AWS customers under NDA. Customers retain control and ownership of their data, thus it is their responsibility to develop auditing procedures for their own environments.
In-Store Branches		O92	Selection criteria should be defined for stores where branches are located	
ATM in convenience store		O93	Selection criteria for store locations should be defined	
		O94	Crime-prevention measures should be implemented during cash loading and other maintenance	
		O95	Procedures for response to failure and disaster should be defined	
		O96	Security measures for network-related devices and data transmissions should be implemented	
		O97	A nitification system should be established for contraction to the police that has jurisdiction and at security companies,etc	
		O98	Take steps to make ATM customers cautions about crime	
Debit Card	**Assure secirity of debit card services**	O99	Security measures should be taken for debit card services	AWS Customers retain the ability and the responsibility to manage financial services security measures for debit card services.
		O100	Assure the security of account numbers, personal identification numbers,etc	
	Customer protection	O101	Measures should be taken to protect customers when they use debit cards	AWS Customers retain the ability and the responsibility to manage financial services security measures for their customers
	Make customers exercise caution	O102	Steps should be taken to make customers exercise caution on certain points regarding the use of debit cards	AWS Customers retain the ability and the responsibility to manage financial services security measures for their customers
Financial Service Using Open Networks	**Internet and mobile services**	O103	Unauthorized use should be prevented	AWS allows customers to manage client and mobile applications to their own requirements.
		O104	Unauthorized use should be detected promptly	
		O105	Conduct information disclosure regarding security measures	
		O105-1	Establish and maintain proper provision for customer services	
		O106	Define Operations management methods	
	E-mail services	O107	Define e-mail operations policy	AWS Customers retain the ability and the responsibility to manage their e-mail operations policy

Major Item	Medium Item	Item No	Minor Item	AWS Response
Measures to Improve Hardware Reliability	**Protection against hardware failure**	T1	Perfom preventive maintenace of hardware	AWS monitors electrical, mechanical, physical security and life support systems and equipment so that any issues are immediately identified. Preventative maintenance is performed to maintain the continued operability of equipment Refer to the "Amazon Web Services Overview of Security Processes" whitepaper available at http://aws.amazon.com/
	Backup for hardware	T2	Provide a standby for a main unit	AWS provides customers the flexibility to place instances and store data within multiple geographic regions as well as across multiple Availability Zones within each region. Each Availability Zone is designed as an independent failure zone. In case of failure, automated processes move customer data traffic away from the affected area. AWS SOC 1 Type 2 report provides further details. ISO 27001 standard Annex A, domain 11. 2 provides additional details. AWS has been validated and certified by an independent auditor to confirm alignment with ISO 27001 certification.
		T3	Provide standbys for peripherals	
		T4	Provide standbys for communications devices	
		T5	Provide backup lines	
		T6	Provide a standby for terminal related devices	
Measures to Improve Software Reliablility	**Measures to improve quality in development phase**	T7	For system development planning,check for proper consistency with medium and long-term planning and obtain proper approvals	AWS applies a systematic approach to managing change so that changes to customer impacting services are thoroughly reviewed, tested, approved and well communicated. Refer to the "Amazon Web Services Overview of Security Processes" whitepaper available at http://aws.amazon.com/
		T8	Include necessary security functions	
		T9	Sofrware quality souhld be assured at design stages	
		T10	Ensure the quality of software in the phase of program development	
		T11	Ensure the quality of software in the phase of testing	
		T12	Ensure the reliablility of software in consideration of program distribution	
		T13	Esnure the quality of package software when installed	
	Measures to improve quality at maintenance stage	T14	Ensure the correctness of routined change operation	AWS performs self-audits of changes to key services to monitor quality, maintain high standards and to facilitate continuous improvement of the change management processes. Refer to the "Amazon Web Services Overview of Security Processes" whitepaper available at http://aws.amazon.com/
		T15	Ensure that the quality of software is maintained even after changing or adding any functions	
Measures to Improve Operational Reliability	**Measures to improve operational r**	T16	Automate and simplify operations	AWS Customers retain the ability and the responsibility to manage operations associated with checking operations.
		T17	Reinforce the function of checking operations	
		T18	Reinforce the function of monitoring and controlling loaded conditions	
		T19	Provide a remote control function for CD/ATM, etc	

Major Item	Medium Item	Item No	Minor Item	AWS Response
Early Failure Detection and Recovery	**Early detection of failures**	T20	Provide the function of monitoring the operational conditions of a system	AWS monitors electrical, mechanical, physical security and life support systems and equipment so that any issues are immediately identified. Customers retain control of their own guest operating systems, software and applications and are responsible for developing logical monitoring of the conditions of these sytems. AWS Cloudwatch provides monitoring for AWS cloud resources and the applications customers run on AWS. Refer to aws.amazon.com/cloudwatch for additional details. AWS also publishes our most up-to-the-minute information on service availability on the Service Health Dashboard. Refer to status.aws.amazon.com.
		T21	Provide the functions of detecting any failures and isolate the points of failure	
	Early recovery from failure	T22	Provide the function for reduction or shutdown and rearrangement of business operations in the event of failures	AWS customers retain control and ownership of their data and associated procedures for managing transfer and revision control of data files. AWS provides customers the flexibility to place instances and store data within multiple geographic regions as well as across multiple Availability Zones within each region. Customers should architect their AWS usage to take advantage of multiple Regions and Availability Zones as distributing applications across multiple Availability Zones provides the ability to remain resilient in the face of most failure modes including natural disasters or system failures.
		T23	Provide the functions of limiting transactions	
		T24	Provide recovery functions from failures	
Disaster Countermeasures	**Backup centers**	T25	Establishment of backup centers	
Data Protection	**Prevention of data leakage**	T26	Take measures not to have personal identification numbers and passwords known by others	The AWS environment is a virtualized, multi-tenant environment. AWS has implemented security management processes, PCI controls, and other security controls designed to isolate each customer from other customers. AWS systems are designed to prevent customers from accessing physical hosts or instances not assigned to them by filtering through the virtualization software. This architecture has been validated by an independent PCI Qualified Security Assessor (QSA) and was found to be in compliance with all requirements of PCI DSS version 2.0 published in June 2011. Refer to AWS Risk and Compliance Whitepaper for additional details - available at http://aws.amazon.com/security.
		T27	Privide the function of identifying a called terminal	
		T28	Take measures for the protection of stored data against disclosure	
		T29	Take measures to prevent leakage of transmission data	
	Prevention of data destruction and falsification	T30	Provide proper exclusive access control to files	AWS customers retain control and ownership of their data and may implement the functions for detecting any defective data.
		T31	Provide the function of contrilling access to files	
		T32	Reinforce the functions of detecting any defective data	
	Detection measures	T33	Take measures for detection of tampered transmitting data	AWS data management policies are in alignment with ISO 27001 standard. Refer to ISO 27001 standard, Annex A, domain 8.2 and 11.3. AWS has been validated and certified by an independent auditor to confirm alignment

Major Item	Medium Item	Item No	Minor Item	AWS Response
		T34	Provide the functions of matching files	with ISO 27001 certification standard. AWS SOC 1 Type 2 report provides additional details on the specific control activities executed by AWS to prevent unauthorized access to AWS resources.
Prevention of unauthorized Use	**Preventive measures(Verify access authorization)**	T35	Set up functions of personal identification	Customers retain the right and responsibility to manage and restrict unautorized use of their IDs. The AWS Identity and Access Management (IAM) service provides identity management features to the AWS Management Console. Refer to the AWS website for additional details - http://aws.amazon.com/mfa.
		T35-1	Examine required security controll measures for biometric authentication in consideration of the characteristics of biometrics	
		T36	Provide the function of preventing unauthorized use of IDs	
		T37	Manage access records	
	Preventive measures (Restrict scope of access)	T38	Provide the function of restricting transactions	AWS customers retain the right and resposniblity to restrict transactions.
		T39	Provide the function of prohibiting transactions when an accident occurs	
	Preventive measures(Unauthorized use and falsification counter measures)	T40	Implement technical precautions against counterfeit card	AWS customers retain the right and responsibility to manage controls and measures for financial cards.
		T41	Set up the protection of electronic value or take measures for detecting unauthorized use of it	
		T42	Provide the function of protecting cryptographic keys to devices and media that store electronic encryption keys, or software included with them	
		T42-1	Provide the function of preventing unauthorized sending/receiveing e-main, or browsing web sites.etc	
	Restriction of access from external networks	T43	Set up functions to protection against unauthorized access from external network	In alignment with ISO 27001 standards, AWS has established formal policies, procedures to delineate the minimum standards for logical access to AWS resources. AWS SOC 1 Type 2 report outlines the controls in place to manage access provisioning to AWS resources. Refer to AWS Overview of Security Processes for additional details - available at http://aws.amazon.com/security.
		T44	Minimize connected devices that can be accessed from external networks	
	Detection measures	T45	Provide the function of monitoring unauthorized access	Customers retain control of their own guest operating systems, software and applications and are responsible for developing monitoring methods for their systems. For AWS systems, In alignment with ISO 27001 standards, AWS has established formal policies, procedures to
		T46	Provide the function of identifying any unusual transactions	

Major Item	Medium Item	Item No	Minor Item	AWS Response
		T47	provide the functions of monitoring exceptional transactions	delineate the minimum standards for logical access to AWS resources. AWS SOC 1 Type 2 report outlines the controls in place to manage access provisioning to AWS resources. Refer to AWS Overview of Security Processes for additional details - available at http://aws.amazon.com/security.
	Responsive measures	T48	Take measures for protection against unauthorized access and of revovering	Customers retain control of their own guest operating systems, software and applications and are responsible for developing monitoring methods for their systems. AWS data management policies are in alignment with ISO 27001 standard. Refer to ISO 27001 standard, Annex A, domain 8.2 and 11.3. AWS has been validated and certified by an independent auditor to confirm alignment with ISO 27001 certification standard. AWS SOC 1 Type 2 report provides additional details on the specific control activities executed by AWS to prevent unauthorized access to AWS resources.
Malicious Program Prevention	**Protective measures**	T49	Take preventive measures against malicious programs such as computer viruses	AWS's program, processes and procedures to managing antivirus / malicious software is in alignment with ISO 27001 standards. Refer to AWS SOC 1 Type 2 report provides further details. In addition, refer to ISO 27001 standard, Annex A, domain 10.4 for additional details. AWS has been validated and certified by an independent auditor to confirm alignment with ISO 27001 certification standard.
	Detective measures	T50	Take proper precautions to detect any computer viruses and other malicious programs	
	Recovery measures	T51	Take measures for cases involving damage from malicious programs such as computer viruses	