Controls Review (cont.)

Question	Yes/No	Comments
3. Are data controllers compelled to periodically verify the accuracy of data, and to update or delete irrelevant/excessive/outdated information?		
4. Are data controllers compelled to communicate the scope of collecting data to the data subject(s)?		
5. Are data controllers compelled to limit the use of data to those communicated to the data subject(s) when the data were collected?		
6. Are data controllers compelled to communicate any change of purpose of collecting/processing data to the data subject(s) and to obtain approval?		
7. Are there limitations to the use of data that forbid any utilization/disclosure not explicitly authorized by the data subject(s)?		
8. Are there requirements about minimum security safeguards requested of the data controllers to protect data against unauthorized disclosure/utilization?		
9. Must data controllers prepare and periodically update a security plan?		
10. Must data controllers periodically conduct a risk assessment?		
11. Are there requirements that make any individual uniquely identifiable and accountable for access to any subject(s) data?		
12. Is the identity of the data controller communicated to the data subject(s) as well as the nature of the data collected/processed?		
13. Are there any training or awareness programs in place to alert staff to the requirements of personal information protection?		
14. Can a data subject(s) ask the data controller for information regarding the existence or nature of data pertaining to him or her?		
15. Can a data subject obtain his or her data from the data controller and verify them?		
16. Is there a maximum period of time fixed to answer questions 15 and 16?		
17. Can a data subject challenge any denial by the data controller to communicate to him or her the existence of data/processing pertaining to him or her?		
18. Can a data subject have the data pertaining to him or her erased by the data controller?		
19. Can a data subject deny at any time to anyone the consent to collect data regarding him or her?		
20. Are there sanctions against data controllers who are not compliant to the above stated principles?		
21. Are there organizations that have a duty to verify compliance of a data controller to the above stated principles?		
Encryption Methodologies		
1. Has management verified that written procedures/policies exist that define the roles and responsibilities for pivotal management control measures, including the following:		

Controls Review (cont.)

Question	Yes/No	Comments
Design Criteria of Cryptographic Systems		
1. Has management verified that the process in which the institution uses to make its choice of encryption algorithms considers the environment where the cryptographic system is to operate including the following:		
a. Type of processing and transmission system to ensure satisfactory integration?		
b. Transmission paths, including compression requirements to guarantee performance service levels?		
c. User's and operator's skills and training to use the system and key?		
d. Integration with the operating environment to ensure communication is secure and reliable?		
e. Algorithm is efficient with regards to the application and its objective?		
2. Has management obtained and reviewed documentation stating that the chosen algorithm ensures the protection at the desired level and is cost effective and convenient for the institution?		
3. Has management collaborated with other IT functions to guarantee minimal effect on interfacing and other system components?		
4. Does management have documentation stating whether the chosen algorithm takes the deciphering cost by an authorized user to a sufficiently cost-prohibitive level?		
5. Is management aware that as computers become more sophisticated and faster, a direct result is the necessity for more complex algorithms and longer keys?		
6. Has management considered and respected the local as well as international laws and regulations?		
7. Has management reviewed documentation stating that the system is strong and not attackable?		
8. Does management know that the security of an effective algorithm does not depend on the secrecy of the algorithm, but rather the secrecy of the keys?		
Change Control Over the Cryptographic System, Including Key Management		
1. Has management verified circa audit testing, that changes and updates to the cryptographic system are controlled and performed by authorized individuals in compliance with existing written policies and procedures?		
2. Is key transmission controlled via a specific procedure?		
3. The inherent risk of having a key disclosed is highest when the key is being transmitted to recipients, to reduce this risk, does the institution currently:		
a. Determine if the retirement of keys based on time is in accordance with the current policy or best industry standards?		
b. Store keys in tamper-resistant modules and never in clear test or programs, where a key's secrecy could become jeopardized without management's knowledge?		

Controls Review (cont.)

Question	Yes/No	Comments
4. Are records maintained to detail who has attended the training, and the level of training received?		
Controls Testing		
1. Do the procedures prescribe who is responsible for setting up the testing of the institution's customer information systems and related system controls and/or procedures by an independent third party?		
2. Are such tests performed at least annually?		
3. Do the tests focus on information system controls, password protection, encryption, procedures, and other relevant elements to protect customer information whether handled in paper format or electronically?		
Independent Third-Party Service Providers		
1. Do the procedures detail the requirements and steps to be followed with respect to dealing with third-party service providers that handle customer information?		
2. Is each service provider reviewed and required to provide the same level of information security protection for customer information as would be required if the function was performed in-house?		
3. Before contracting with an independent third-party service provider, does the information security officer perform a due diligence review of the vendor's information security controls and procedures?		
4. As part of the outsourcing contract, are vendors required to be familiar with the institution's customer information security requirements and, therefore, maintain the outsourced services under the same level of control(s)?		
5. Do the procedures require that the vendor continue to monitor information security controls and advise the institution of the level of risk associated with the services provided?		
6. Are vendor audits and internal reviews that are relevant to the contracted customer information services provided to senior management?		
7. Is a list maintained of all customer information service providers, their names, addresses, services provided, and assigned risk rating regarding information security?		
Storage		
1. Are procedures detailed regarding the protection of customer information that is stored offsite for records retention purposes?		
2. Do the procedures describe levels of security and requirements to allow only authorized individuals access to stored information?		
3. Are customer information records storage procedures reviewed to ensure proper backup exists?		