System Validation & Compliance
Example Technology Solutions

	S e c u r i t y
1	Access limited to authorized individuals (roles and privileges defined by data owners)
2	No users with "God" role – i.e., no remote IT people with user system administrator role
3	Password minimum length of 8 characters
4	Password makeup requirements (no words in dictionary, alphanumeric)
5	Password change frequency of 90 days
6	Password reuse frequency of 1 year
7	Passwords not displayed when entered
8	Passwords not remembered by browsers and applications
9	Password only known by individual user
10	Password encryption upon entry, storage
11	Password cannot be copied and pasted
12	Passwords are not e-mailed or written down
13	Passwords are not shared
14	Temporary passwords are unique
15	Temporary passwords must be changed at next log-on
16	Temporary password expires in 24 hours
17	User name appears on screen
18	User name is unique
19	User name identifies a person, not generic
20	User name is not deleted, just inactivated and therefore, cannot be reused.
21	Automatic log-off after inactivity of 10-20 minutes.
22	OS screen saver with password of 10-20 minutes
23	Auto-lockout after too may failed log on attempts; e-mail notification to system administrator/security staff after 3-5 attempts
24	All user activity is logged
25	When logging onto a system from a second location, both users are notified
26	Automatic lock-out of inactive accounts of 30 days or more
27	Last log-on is displayed when logging on
28	Network security in place for internet, virus protection, physical security
29	Removable media, including laptops and PDAs, have confidential data encrypted
30	Device checks confirm that once data starts from a device, another device doesn't take over
	D a t a T r a n s f e r
31	Limited and controlled delete capabilities
32	Data transferred outside of the intranet firewall is encrypted
33	Data taken off site is encrypted (laptops, removable media)
34	System includes operational checks to enforce correct sequencing of events and validity of input data
35	Date format so that month and day are discernable (i.e., 10 Jan 2009, where Jan is alpha-characters)
	A u d i t T r a i l
36	Audit trail records the creation, modification, or deletion of electronic records
37	Record user name, date, time, previous data, new data, and reason for the change (if required by predicate rules)
38	Users can access the audit trail
39	Indication of changed data is known to the user by on-screen indication, not just in audit trail
40	All computers must be synchronized to a standard time source
41	Application aware that data integrity has been compromised; database encryption, record checksums, backend changes written to audit trail