9.3 Data states

9.3.1 At rest

Item	*Rate*
Physical security measures associated with the storage location act as a significant part of the protection afforded to that data.	
Tapes are disconnected from any computing device and only come in contact with those devices when passing by the tape head that reads or writes them.	
Tapes are manipulated using robotic devices to move them between large storage areas and tape readers and writers. Those readers and writers are most often disconnected from the computers that use them and they are accessed at a distance over internal cabling.	
Tapes are large enough that they have to be concealed with something else that is noticeable in order to be removed	
Tapes have bar codes or other similar markings to allow them to be identified and tracked, and are stored within hardened data centers or other similar areas.	
Tapes are missed in periods of hours to days when illicitly removed.	
Tapes are read every few years in order to be refreshed,	
Tapes are kept in climate controlled environments at all times.	
Alarms identify environmental changes with enough time to mitigate harm to tapes.	
Disks are kept within cases inside systems	
Physical access to disks is time rated.	
Disks are replaced every 3-5 years if they have not failed.	
Old disks are destroyed instead of being resold.	
Paper storage is controlled, marked, tracked, and accounted for.	
Duplicates of important paper records are kept either in paper form or in electronic scanned form.	
Duplication machines are controlled so that important records cannot be FAXed, duplicated, or otherwise taken easily without proper authorization.	
The control scheme classifies paper records and restricts access to authorized users with appropriate clearances.	
Physical security measures assure that paper records are protected to a level commensurate with the risks of access.	
Paper records containing financial information, health related information or other information controlled by regulatory or contractual requirements are protected commensurate with those requirements.	
Fiche is protected similarly to paper records except that more information is contained per unit of space and susceptibility to different environmental conditions dictates different risk analysis values.	
Inventories of fiche and paper track them throughout their life cycles.	

Item	***Rate***
Disposal and destruction of fiche and paper records are handled commensurate with their value.	
Portable digital media is not used for high valued information.	
Systems containing high-valued information do not have usable interfaces to removable storage media.	
Media-specific processes are used to assure operation over long times	
Legal requirements for data retention associated with business records and the requirements associated with data retention policy are implemented for all stored data.	
Protection of data at rest is facilitated by operating system access controls.	
Availability is assured by redundancy with redundant disk storage as a local solution.	
Availability is assured by redundancy with distributed backups, checkpoints, and transaction records as a solution for transaction systems, databases, and file systems that support this sort of change mechanism.	
Accountability is retained by ownership records associated with data.	
Accounting data is retained locally if adequate system protection is available or write once read many (WORM) disks are available for this purpose.	
Total ratings and divide by 29	

Startup	***Diligence***	***Typical***	***Excellent***	***Best***
1	5	6	7	9

9.3.2 In motion

Rate each area from 0 to 10. Sum the ratings and divide by 15 for a total.

Item	*Rate*
If the physical security of the transmission media is adequate to the need, no additional measures are required.	
If insecure infrastructure is used, additional protection is used as consequences increase.	
In push systems the sender is responsible for providing appropriate protection.	
In pull systems servers take into account the user request and authorization based on identification and authentication to determine and apply the proper protection to the situation.	
Encryption is used to protect medium and high valued information in transit.	
Secure socket layer (SSL) encryption is used for confidentiality protection of medium risk data transfers when feasible.	
Cryptographic protocols and algorithms are analyzed for transmission of high valued information and risk management determines requirements for these protocols and algorithms.	
Transmission over multiple channels and paths for path and channel diversity is used for high valued information.	
Spread spectrum is used for increased reliability for radio transmissions.	
Transport media dictates protective measures through risk management.	
Tapes and similar media is protected in transport to the level of surety appropriate for the data being protected.	
Verification of transmitted information is done using cryptographic checksums.	
Verification of syntax, form, and values in context of the receiving system is required for all transmitted information.	
Separation is used between different surety levels to assure non-interference in transmitted data.	
Adequate bandwidth and quality of service controls are in place to assure control and audit information can pass and be processed.	
TOTAL (add ratings and divide by 15)	

Startup	*Diligence*	*Typical*	*Excellent*	*Best*
1	5	6	7	9.5

9.3.3 In use

Rate each item from 0 to 10. Sum the ratings and divide by 10 for overall rating.

Item	*Rate*
Data is validated before use.	
Input is always validated for syntax and value ranges based on program state.	
Inconsistencies are detected and fail safe operation modes are used when inconsistencies are detected.	
Verification is used to increase the surety level associated with medium and high valued data.	
Submit-commit cycles are used in transaction systems to cover high valued transactions.	
Redundant processing is used to increase surety of results for high risk situations.	
Processing uses checksums or state verification mechanisms to assure that transformations produce appropriate output for high risk situations.	
Data in use is protected from other processes by hardware process separation at the operating system or physical device level.	
Reconciliation is used to verify consistency of results.	
Protective mechanisms and classification controls are maintained for all instances of data in use.	
TOTAL (Sum the ratings and divide by 10 for a total.)	

Startup	*Diligence*	*Typical*	*Excellent*	*Best*
2	5	5	7	9

9.3.4 Roll-up

State	*Rate*	*Level*	*Startup*	*Diligence*	*Typical*	*Excellent*	*Best*
At Rest			1	5	6	7	9
In Motion			1	5	6	7	9.5
In use			2	5	5	7	9
TOTAL / 3			1.33	5	5.66	7	9.16

Enter ratings from above and divide by 3 for the total. Rate each area's level by selecting the highest level not exceeding the rating.