9.2.4 Data

Rate each issue from 0 to 10 for low, medium, and high surety systems.

9.2.4.1 Inception

Item	*L*	*M*	*H*
Limitations on cognitive input capacity are taken into account when attributing security properties to inputs.			
Enter rating from above			

9.2.4.2 Observation

Item	*L*	*M*	*H*
Sensor and interpretation capabilities and limits are considered when attributing security properties to inputs.			
Source and path of observation are considered in associating properties with observations.			
Total ratings and divide by 2			

9.2.4.3 Entry

Item	*L*	*M*	*H*
Entry errors and limitations are considered in associating properties with observations.			
Enter rating from above			

9.2.4.4 Validation

Item	*L*	*M*	*H*
Validation processes are used to check for proper syntax, limits, and internal consistency of inputs.			
Syntax checks are used to validate inputs so that no illegitimate or invalid input for the application in context is accepted.			
Validation includes limits on length, value, symbols and symbol sequences, and all of these in the context of program state.			
Limits are used to prevent excesses based on policies or design.			
Inputs with redundancy, such as the entry of a postal code and state in a form are checked for consistency at input.			
Total ratings and divide by 5			

9.2.4.5 Verification

Item	*L*	*M*	*H*
Verification is used to confirm or refute data values.			
Verification uses a separate and different method of confirmation than the original source and process.			
The level of verification depends on costs associated with verification and risks associated with the use of unverified data through the risk management process.			
Total ratings and divide by 3			

9.2.4.6 Attribution

Item	*L*	*M*	*H*
Attribution associates the physical input channel to the data.			
Attribution associates data with the system or hardware device that provided it.			
Attribution associates data with its human source and the individual responsible for its entry.			
Attribution associates the organization behind data with that data.			
Attribution is associated with a level of trust.			
Total ratings and divide by 5			

9.2.4.7 Fusion

Item	*L*	*M*	*H*
Tracking of fused data to reflect aggregation effects is used to assure that the security architecture is properly implemented in fused content.			
Tracking of identities and attributes associated with fused data is done.			
Total ratings and divide by 2			

9.2.4.8 Separation

Item	*L*	*M*	*H*
Separation requirements associated with data are generated through the risk management process.			
Data separation is enforced by zoning implementation.			

Item	*L*	*M*	*H*
Data is only accessible to users when the user clearance is commensurate with the data classification.			
Functions performed are limited based on the needs of the user with respect to the data.			
Total ratings and divide by 4			

9.2.4.9 Analysis

Item	*L*	*M*	*H*
Analysis of data is verified to produce meaningful content for the application.			
Error, error propagation, and sensitivity analysis are used to limit business consequences of errors.			
Total ratings and divide by 2			

9.2.4.10 Transforms

Item	*L*	*M*	*H*
Integrity of standardized transforms is verified before being made available for use.			
Enter rating from above			

9.2.4.11 Transmission, Storage, and Use

Item	*L*	*M*	*H*
Transmission is generally associated with the data in motion state as described elsewhere.			
Storage is generally associated with the data at rest state which is described elsewhere.			
Use of data is generally associated with the data in use state described elsewhere.			
Total ratings and divide by 3			

9.2.4.12 Presentation

Item	*L*	*M*	*H*
Presentation of data accurately represent the intents of the application.			
Enter rating from above			

9.2.4.13 Modification

Item	*L*	*M*	*H*
Accidental modification of data is covered by statistically verifiable controls such as redundancy and fault tolerance.			
Intentional and appropriate modification is properly handled and assured to the risk levels involved.			
Malicious modification of data is mitigated by cryptographic checksums or other redundancy for detection where risks are medium or high.			
Malicious modification of data is prevented by access controls.			
Total ratings and divide by 4			

9.2.4.14 Loss

Item	*L*	*M*	*H*
Redundancy to the risk management specified level protects against loss of utility.			
Encryption or prevention from physical access even when in possession of the data's container is used to mitigate against data loss.			
Total ratings and divide by 2			

9.2.4.15 Recovery

Item	*L*	*M*	*H*
Data with substantial value is backed up or otherwise kept, sent, or created redundantly.			
Data that can be inexpensively regenerated may not be backed up.			
Data recovery from broken or failing media is performed when data is valuable and inadequate backup is available.			
Insurance is used to transfer risk of data loss when other techniques are less cost effective.			
Legal process is used for recovery when civil actions are cost effective.			

Item	L	M	H
Specialized expertise in data recovery, forensics, investigative, or law enforcement processes are used when appropriate.			
Total ratings and divide by 6			

9.2.4.16 Reconstruction

Item	L	M	H
Reconstruction of data is used if fragments exist at different places, or if the original values can be derived from data values associated with or derived from them.			
Enter rating from above			

9.2.4.17 Backup

Item	L	M	H
Backup is a fundamental process used to assure availability over time.			
Different sorts of backup are used based on timeliness, redundancy, transportation, quantity, and duration issues.			
For data that has to be restored from backups in near real time, duplicate (hot standby) systems are used.			
For data that has to be highly redundant, the redundancy requirement leads to the number of copies and their diversity in space and media.			
For data in large quantity or that has to be at distant locations in some time frame, media and bandwidth are determined to meet the need.			
For backups required to last different amounts of time, different storage media and processes are used.			
For typical data, typical backup regimens include daily incremental backup of changed data kept for one week, weekly incremental or full backups of all data kept for a month, monthly full backups kept for a year, and annual full backups kept indefinitely or retained for the legally mandated duration for business records.			
Backups are tested by restoration on a regular basis to assure viability.			
Backups are protected to the same surety as systems they back up.			
Total ratings and divide by 10			

9.2.4.18 Restoration

Item	*L*	*M*	*H*
Restoration from backups is tuned to the backup process.			
Restoration process is tuned to media and timeliness requirements.			
Total ratings and divide by 2			

9.2.4.19 Destruction

Item	*L*	*M*	*H*
Destruction of data is tuned to the media and surety requirement.			
For digital data stored on disk or tape, deletion of files is used only for low risk situations.			
Secure deletion based on multiple pattern-based overwrites is used in cases where medium or high grade threats are active.			
Electromagnetic erasure with high Oersted field generators is used for medium risk situations.			
Physical destruction of disks is used only for high risk levels.			
Physical destruction of the media and its contents by burning at high temperatures for a long enough time or boiling in acid of the proper type for a long enough time is used for high risk data on digital storage.			
Strip shredders are never used for paper destruction.			
Cross-cut shredders at a few square millimeter shred sizes are used for typical printouts.			
Sensitive and non-sensitive data are joined together in shred bins to increase volumes.			
Shredding is done by the individual at the point of disposal.			
Disposal for medium and high risk paper-based data uses cross-cut shredding of the proper size, then uses burning or pulping with a recycling process under physical control of trusted cleared personnel.			
For CD-ROMs and Fiche with high valued data, destruction is done by burning or emulsifying with acid.			
For rapid initial destruction of CD-ROM data, a microwave oven or shredder is used prior to the normal disposal process under proper health and safety protections.			
Total ratings and divide by 13			

9.2.4.20 Roll-up

Item	*L*	*M*	*H*
Inception			
Observation			
Entry			
Validation			
Verification			
Attribution			
Fusion			
Separation			
Analysis			
Transforms			
Transmission			
Storage			
Use			
Presentation			
Modification			
Loss			
Recovery			
Reconstitution			
Backup			
Restoration			
Destruction			
Sum columns and divide by 21			

Risk	*Startup*	*Diligence*	*Typical*	*Excellent*	*Best*
Low	0	2	2	2	2
Medium	1	4	4	6	7
High	2	8	4	6	9