8 Control architecture

8.1 Protection objectives

8.1.1 Integrity

Rate each item for low, medium, and high risk systems. Sum the ratings and divide by 20 for aggregate ratings.

Area	*L*	*M*	*H*
In most cases, the integrity of information is most important to its utility.			
Source integrity is rated and required for access to medium and high valued systems.			
Cryptographic technologies are used to detect unauthorized change.			
Sound change control protects networks, systems, and applications.			
Redundancy is used to detect and, in some cases, correct faults.			
Validation and verification processes are used for code.			
Consistency checks use redundancy to validate data.			
Validation and verification processes are used for data.			
Multi-source verification is used.			
Multi-factor approaches are used to independently verify content.			
Trust models are created and applied to provide metrics on trust.			
Submit/commit cycles provide separate channel confirmation.			
Watermarking is used to provide a self-validation of media.			
Cryptographic checksums provide redundancy that allows validation of use of specific keys or confirmation of content against published coded values.			
Integrity shells are used to detect unauthorized program changes.			
Digital signatures are used to validate content.			
Certificates are used to provide validation of the authority to sign.			
TCSEC systems are used to assure flow control.			
TCG systems are used for integrity protection.			
Integrity of personnel is considered in background checks.			
TOTAL (sum ratings and divide by 20)			

	Startup	*Diligence*	*Typical*	*Excellent*	*Best*
Low surety	0.1	1	2	3	4
Medium surety	1	2	2	4	7
High surety	2	5	5	7	9

8.1.2 Availability

Rate each item for low, medium, and high surety systems from 0 to 10. Sum the items and divide by 10 for an overall rating.

Item	*L*	*M*	*H*
Risk management defines availability consequences as a function of time.			
Availability is measured in terms of mathematical formulas.			
Interdependency analysis is used to determine availability of systems based on availability of other systems they depend on.			
Redundancy is used to increase availability by making independent resources available in case of failure.			
Redundancy is carefully implemented to avoid brittleness			
Redundancy is carefully implemented to avoid common mode failures.			
Higher quality components are used to increase availability.			
Availability is measured as part of the enterprise feedback system.			
Availability is rated as more or less critical for different systems.			
Disaster recovery and business continuity planning assure availability.			
TOTAL (sum ratings and divide by 10)			

	Startup	*Diligence*	*Typical*	*Excellent*	*Best*
Low surety	1	2	2	4	6
Medium surety	3	6	4	7	8
High surety	4	8	6	8	9

8.1.3 Confidentiality

Rate each item for low, medium, and high surety systems from 0 to 10. Sum the items and divide by 12 for an overall rating.

Item	*L*	*M*	*H*
Confidentiality is controlled based on clearance of identity, certainty of authentication of identity, classification of content, and need for use.			
The means of creating and operating this basis is protected to the level of the information it protects.			
Information flow controls are used to limit the movement of information from place to place.			
Network and system separation are used to prevent mixing of data of different confidentiality.			
Separation controls are implemented at routers through network separation technologies (e.g., VLANs with quality of service controls)			
Separation controls are implemented within computer systems through access controls.			
Separation mechanisms are implemented between networks by distance and with shielding.			
Separation mechanisms are implemented in applications through application-level access controls.			
TCSEC systems are used for separation with risk management defining the TCSEC rating associated with information classification.			
Cryptography is used as a separation mechanism to prevent those who gain access to data from meaningfully using the content it represents.			
Abyss processors and similar containment devices are used for high surety processing.			
Digital diodes are used for one-directional information flow.			
TOTAL (sum rates and divide by 12)			

Risk level	*Startup*	*Diligence*	*Typical*	*Excellent*	*Best*
Low surety	1	3	3	4	4
Medium surety	2	6	6	7	9
High surety	4	8	6	9	9.5

8.1.4 Use control

Area	*L*	*M*	*H*
Use control associates authentication requirements with identified parties for authorized uses.			
Only identified individuals or systems acting on their behalf are granted appropriate use based on their identity and the extent to which they have demonstrated that identity to be authentic.			
If the current level of authentication is inadequate to the need, additional authentication is required to meet the level required for the use.			
Biometrics are used to provide authentication based on physical characteristics typically associated with individuals out of a group.			
Other authentication technologies such as smart cards, tokens, universal serial bus (USB) authentication devices, proximity cards, radio frequency identification (RFID) tags, and so forth are used as proof of something the user possesses.			
Passwords, pass phrases, or similar methods based on user knowledge, skills, and capability indicate something the user knows or can do.			
Separation of duties is implemented as a use control			
Separation of duties is operated with consideration of time transitivity.			
Time transitivity controls and relationships are tracked in use controls.			
Life cycle tracking of individuals is employed in use control.			
Use control interacts with roles through HR-related limitations.			
Process controls limit how processes can proceed.			
Separation of duties is applied to systems administrators of systems that must be independently operated.			
Change control personnel are kept separate from developers and operators.			
Operators are kept separate from change control and developers.			
Developers are kept separate from change control and operators.			
Submit/commit systems are used as control devices to separate the preparation of a transaction from its approval process.			
Commit devices are separate, different, and independent of submit devices.			
Roles and rules implement use control at the management level.			
Identity management (IdM) infrastructure is used for administration.			
Risk aggregation associated with IdM is managed properly to the risk.			
TOTAL (sum the ratings and divide by 21)			

Risk level	*Startup*	*Diligence*	*Typical*	*Excellent*	*Best*
Low surety	1	3	3	4	4
Medium surety	2	6	6	7	9
High surety	4	8	6	9	10

8.1.5 Accountability

Rate each item from 0 to 10 for low, medium, and high surety systems. Sum items in each column and divide by 18 for a total.

Item	*L*	*M*	*H*
Accountability tracks attribution of actions to actors.			
Accountability accurately identifies and records event sequences of interest.			
Accountability accurately associates activities with actors in situations.			
Identity and surety information associated with authentication processes is used to assert attribution.			
Individuals associated with identities are registered in a process with identified and tracked surety characteristics.			
Audit trails are generated by mechanisms with identified surety levels.			
Audit trails are transported by mechanisms with identified surety levels.			
Audit trails are stored in write-once read-many storage mechanisms.			
Audit retention is defined by legal and risk management requirements.			
Audit information is transferred only through authorized and properly protected means.			
Audit information cannot be altered when examined or analyzed.			
Audit systems are protected to the level appropriate to the information they collect, transport, and store.			
Analysis of audit system designs includes risk and data aggregation effects.			
Audit records are separated from data and control.			
Audit trail granularity is determined by risk management.			
Audit records are correlated across platforms for validity and consistency.			
Audit records are kept in time bases that are reconcilable for definitive timing information.			
Missing or excessive audit records are identified and investigated.			
TOTAL (sum columns and divide by 18)			

Risk level	*Startup*	*Diligence*	*Typical*	*Excellent*	*Best*
Low surety	1	5	3	6	8
Medium surety	2	6	6	7	9
High surety	3	8	7	9	10

8.1.6 Roll-up

Ares	*Risk Level*	*Rate*	*Level*	*S*	*D*	*T*	*E*	*B*
Integrity	Low			0.1	1	2	3	4
	Medium			1	2	2	4	7
	High			2	5	5	7	9
Availability	Low			1	2	2	4	6
	Medium			3	6	4	7	8
	High			4	8	6	8	9
Confidentiality	Low			1	3	3	4	4
	Medium			2	6	6	7	9
	High			4	8	6	9	9.5
Use Control	Low			1	3	3	4	4
	Medium			2	6	6	7	9
	High			4	8	6	9	10
Accountability	Low			1	5	3	6	8
	Medium			2	6	6	7	9
	High			3	8	7	9	10
TOTAL LOW / 5				0.8	2.8	2.6	4.2	5.2
TOTAL MEDIUM / 5				2	3.2	4.8	6.4	8.4
TOTAL HIGH / 5				3.4	7.4	6	8.4	9.5