9.6 Protective mechanisms

9.6.1 Perception

Rate each item from 0 to 10. Sum the ratings and divide by 20 for a total rating.

Item	*Rate*
Perception-related defenses are used to influence specific threats.	
Key computing facility locations and functions are kept obscure.	
People engaged in sensitive activities are kept obscured through an operations security program.	
Locations of key executives and times and places of their meetings is kept obscure.	
Locations of key systems are kept obscure.	
Other key elements of critical information infrastructure are kept obscure.	
Obscurity is systematically applied to limit knowledge of high valued systems and content by those without a need to know it.	
High valued targets are put in low profile locations to reduce the likelihood of non-directed attacks from impacting them.	
Buildings that have data centers are not be marked as such.	
Computer centers with large glass walls in imposing spaces are not used.	
Locations of critical data centers are protected by an operations security program.	
Names and locations of financial and critical systems are kept obscure.	
Public relations works to eliminate negative impressions of the enterprise in general and specifically addresses the views of likely threats to information and systems.	
Specific public relations efforts are addressed at threats to the industries the enterprise participates in.	
The appearance of a direct effect on the set of threats that are likely to be faced is avoided and actively countered by public relations.	
Deceptions are directed to exploiting error mechanisms in target threat sets and designed to not interfere with normal operations.	
Firewall deception capabilities are used where available.	
Password deception mechanisms are used where available.	
Other built-in deceptions are used where available and non-harmful.	
Complex deceptions are only used when the risks justify the increased costs and complexities.	
TOTAL (sum the ratings and divide by 20)	

Startup	*Diligence*	*Typical*	*Excellent*	*Best*
1.8	5	5	7	10

9.6.2 Structure

Rate each item from 0 to 10. Sum the ratings and divide by 17 for a total rating.

Item	*Rate*
The structure of networks, systems, applications, facilities, and businesses are effectively used to limit risks.	
Structural mechanisms are used to create structures that provide some number of layers of defense against attacks from different sources.	
Structural defenses are used to separate zones based on common perimeter needs and limitation of risk aggregation.	
Mandatory access controls are used for matching protection mechanisms to access control requirements of the control architecture in medium and high surety applications.	
Discretionary access control is only relied on for low surety separation.	
Information flow limitations are used to form barriers between zones.	
Virtual local area network (VLAN) technologies with rate shaping are used to separate area of networks.	
Router-based controls are used to limit network addresses, physical interfaces, and network ports across routers or switches.	
Rate limits on network are used to limit denial of services attacks.	
Routing is used to force specific traffic to travel along specific routes.	
Digital diodes and similar mechanisms are used to provide high assurance that information can only go where it is supposed to go.	
Covert channels are controlled in high surety systems.	
Firewalls and similar permeable barriers are used to limit the effects of issues on one side of the barrier from impacting other sides of the barrier while still allowing select information to pass.	
Firewalls implement demilitarized zones (DMZs) and/or proxy servers to limit packet-level and transport-level attack mechanisms if performance and cost allow.	
If performance or cost prevent the use of proxy servers or similar low-level attack limiters then the systems accessed through the firewall are designed to prevent serious negative impacts from these mechanisms.	
Firewalls are used to allowed authorized protocols, ports, addresses, and to a lesser extent sub-protocol elements, and prevent other traffic.	
Network address translation (NAT) is used in firewalls where possible to limit unauthorized routing.	
Intrusion and anomaly detection designed to verify firewall operation are used when risks justify them.	
Intrusion and anomaly detection designed to verify firewall operation are independent of the firewalls they verify.	
TOTAL (sum the ratings and divide by 17)	

Startup	*Diligence*	*Typical*	*Excellent*	*Best*
1.8	5	5	7	10

9.6.3 Content controls

Rate each item from 0 to 10. Sum the ratings and divide by 11 for a total rating.

Item	*Rate*
Separation mechanisms are used for low, medium, or high surety separation based on proper configuration, control, and use.	
Transforms are used for medium or low surety protection based on proper configuration, control, and use.	
Filters are used only for low surety protection.	
Encryption of content is used to make it meaningless if examined.	
Digital signatures are used for increased assurance of detection if modified	
Digital rights management software is used for low surety protection only.	
Virtual private networks (VPNs) are used for medium or low surety extension of zones across infrastructure.	
Transforms are used on markings associated with content to reflect changes associated with functions performed on the content in medium or high surety systems.	
Filters are used as a low surety mechanism to limit what is allowed to pass.	
Known virus, spam, spyware, Trojan horse, and similar detectors are only trusted for low surety protection.	
Unauthorized syntax and data sequence detectors are used only as low surety mechanisms to prevent content from passing outward.	
TOTAL (sum the ratings and divide by 11)	

Startup	*Diligence*	*Typical*	*Excellent*	*Best*
1.8	5	5	7	10

9.6.4 Behavior

Rate each item from 0 to 10. Sum the ratings and divide by 27 for a total rating.

Item	*Rate*
Behavioral mechanisms are used to deal with situations that can be detected by external observation, situations in which behavioral limits can be set regardless of the content or its use, or situations in which controlling behaviors facilitates protection.	
Change detection and prevention implement enterprise control architecture functions.	
Read-only media is used to limit changes where feasible.	
Bootable CD-ROMs are used to provide high assurance against changes in the operating environment.	
Change detection is used for verifying change controls over programs in medium and high surety systems.	
Control over times and rates are used in behavioral detection systems.	
Rate controls are used to limit how much happens in a period of time.	
Rate controls are used to protect critical servers against denial of services.	

Item	*Rate*
Failure modes that can be identified in advance and safe modes for operation in those moides are used for medium and high surety systems.	
Programmable logic controllers are used to provide for fail safe in protecting critical systems in medium and high surety situations.	
Fault tolerant computing is used when faults are unavoidable but failure is too harmful.	
Uninterruptible power supplies are used for systems in which short term outages are too high consequence to tolerate.	
Motor generators are used for systems in which long-term power outages are harmful.	
Hot stand bye systems are used when momentary failure is unacceptable.	
Warm stand bye systems are used when rapid recovery is required.	
Adequate distance, separation, and other protective measures are used to assure that redundant systems are protected from common mode failures.	
Intrusion detection is used to detect event sequences with potentially serious negative consequences in time to mitigate those consequences to an acceptable degree.	
Anomaly detection systems are used to detect changes in behavior that are outside of the normal changes associated with the operation of the system under examination.	
Response systems are designed and implemented to prevent the serious negative consequences detected by intrusion and anomaly detection systems.	
Detection and analysis of human behaviors and behavioral changes are used to identify situations in which investigation is to be undertaken.	
Separation of duties is used to limit behaviors in excess of management-defined risk thresholds.	
Submit-commit cycles are used when independent verification over time is suitable to the need to separate duties or to mitigate harmful effects of attacks on single or low surety systems.	
Multiple approvals before performing a dangerous operation are used in cases where risk management thresholds exceed management mandates.	
Separation of duties is used when insiders become too powerful for risk aggregation limits specified by executive management.	
The principle of least privilege is used in all medium and high risk situations to limit effects of individuals, processes, and programs.	
Server programs give up privilege when not needed and are designed to only use privileges are necessary at startup.	
Behavioral mechanisms suitable to the surety level desired are applied.	
TOTAL (sum the ratings and divide by 27)	

Startup	*Diligence*	*Typical*	*Excellent*	*Best*
1.8	5	5	7	10