7.3.6 Technical safeguards - Informational

Rate each issue from 0 to 10 then add up the results in each area then add the totals and divide by 15 for an overall rating.

7.3.6.1 General

Issue	*Rate*
Specific defenses are applied to reduce threats.	
Specific defenses are applied to reduce the link between threats and vulnerabilities.	
Specific defenses are applied to reduce vulnerabilities.	
Specific defenses are used to reduce the link between vulnerabilities and consequences.	
Specific defenses are applied to reduce consequences.	
Defenses are used to sever specific attack sequences.	
Defenses are selected based on the event sequences they are intended to mitigate.	
Defense redundancy is used to protect higher risk systems with redundancy dictated by risk management.	
Defense-in-depth is practiced throughout the enterprise.	
Power and disk redundancy is used for high availability.	
Integrity protection is used in almost all systems.	
Availability protection is used when risk management justifies it.	
Confidentiality protection is used when risk management justifies it.	
Use control is applied in all cases based on protection architecture.	
Audit is used in all cases.	
Control is separated from data.	
Audit is separated from data and control.	
Interdependency analysis is used in non-low risk systems.	
Risk aggregation is analyzed and applied for all systems.	
Fail safes are used for non-low risk situations.	
TOTAL THIS AREA / 20	

Copyright © 1977-2005 Fred Cohen & Associates – All Rights Reserved

7.3.6.2 Mainframes

Issue	*Rate*
Access controls based on user identity are used.	
Subject/object models are used to codify protection.	
Sound change control is used.	
Standardized audit is used.	
Limited function user interfaces are used.	
Query limits are used in databases.	
Redundant system capabilities are used.	
Separation of duties is used.	
System security levels match risk levels.	
RACF, ACF2, Top Secret or a similar secure operating system is in use.	
TOTAL THIS AREA / 10	

7.3.6.3 Midrange

Issue	*Rate*
Access controls based on user identity are used.	
Subject/object models are used to codify protection.	
Sound change control is used.	
Standardized audit is used.	
Limited function user interfaces are used.	
Query limits are used in databases.	
Redundant system capabilities are used.	
Separation of duties is used.	
System security levels match risk levels.	
TOTAL THIS AREA / 9	

7.3.6.4 Servers

Issue	*Rate*
Power and disk redundancy is used.	

Copyright © 1977-2005 Fred Cohen & Associates – All Rights Reserved

Issue	*Rate*
Access controls based on user identity are used.	
Subject/object models are used to codify protection.	
Sound change control is used.	
Standardized audit is used.	
Limited function user interfaces are used.	
Query limits are used in databases.	
Redundant system capabilities are used.	
Separation of duties is used.	
System security levels match risk levels.	
TOTAL THIS AREA / 10	

7.3.6.5 Clients

Issue	*Rate*
Low surety platforms are used only for clients in low risk situations.	
Medium surety clients are used in medium risk situations.	
High surety clients are used in high surety situations.	
Separation is used to increase surety associated with low surety clients in non-low risk areas.	
Thin clients are used when feasible for high surety systems.	
TOTAL THIS AREA / 5	

7.3.6.6 Firewalls

Issue	*Rate*
Firewalls or digital diodes separate areas in the perimeter architecture.	
Firewalls are used as separation devices between enclaves.	
Firewalls are used as perimeters for individual computers.	
Firewalls limit addresses, protocols, and content.	
TOTAL THIS AREA / 4	

Copyright © 1977-2005 Fred Cohen & Associates – All Rights Reserved

7.3.6.7 Networks

Issue	*Rate*
Networks use virtual LANs to separate services.	
Networks use quality of service (QoS) controls to guarantee separation.	
QoS is used to guarantee control is separated from data.	
QoS is used to guarantee audit is separated from data.	
QoS is used to guarantee adequate bandwidth for non-low surety traffic.	
Network control is operated at high assurance levels.	
Networks are operated by highly trusted individuals.	
Network controls implement security architecture.	
TOTAL THIS AREA / 8	

7.3.6.8 Telephony

Issue	*Rate*
Voice over IP (VoIP) is used for reduced cost in low surety applications.	
Voice over IP is in separate VLANs from other IP traffic.	
VoIP is protected by QoS controls to assure bandwidth.	
VoIP is encrypted for medium and high surety networks.	
Control is separated from data in voice communications.	
TOTAL THIS AREA / 5	

7.3.6.9 Backbone

Issue	*Rate*
Risk aggregation for backbones is analyzed.	
Physical security protects all backbones.	
Backbone protection is dictated by risk management.	
Encryption is used to protect backbone communications.	
TOTAL THIS AREA / 4	

Copyright © 1977-2005 Fred Cohen & Associates – All Rights Reserved

7.3.6.10 Cabling

Issue	*Rate*
Cables are protected commensurate with the levels of data flowing through them.	
Cable rooms are protected commensurate with the highest consequences associated with data flowing through them.	
Cables are separated based on surety requirements.	
Data cabling is separated from electrical cabling.	
Redundant cabling between sites through separate routes is provided for availability.	
Infrastructure analysis is used to assure redundancy in cables.	
People working on cables are cleared to the level of the data running through those cables.	
TOTAL THIS AREA / 7	

7.3.6.11 Hosts

Issue	*Rate*
Host protection is based on risk management associated with the risk level of the system.	
Mobile hosts are prevented from containing unencrypted data of more than low consequence.	
Hosts in medium and high surety levels are physically secured and inventoried.	
Networked hosts are protected with host-based firewalls.	
Surety of hosts matches risks of their content and use.	
TOTAL THIS AREA / 5	

7.3.6.12 External links

Issue	*Rate*
All external links are protected by firewalls.	
All non-low risk external links are protected by encryption.	
External links are controlled to limit the locations they can reach in internal networks.	
External links are approved by owners of all systems they attach to.	

Copyright © 1977-2005 Fred Cohen & Associates – All Rights Reserved

Issue	*Rate*
Users with external access to non-public information are controlled through the same architectural elements as internal users.	
External outbound connections are only allowed from low risk systems.	
Only low risk systems can be accessed directly from external links.	
Paths from external links to medium risk systems pass through protective barriers and can only be indirect.	
Paths from external links to high risk systems must pass through medium surety systems first.	
All external links to medium or high risk systems have risk management approval for technical protections.	
TOTAL THIS AREA / 10	

7.3.6.13 OS's

Issue	*Rate*
Operating systems protection is used where available.	
Operating system protection is preferred over application-level protection.	
Risk management approves operating systems for non-low risk systems.	
Operating system encryption is used on non low risk mobile systems.	
Standards for operating system protection are approved by risk management.	
Operating systems are updated when they require services with known exploitable faults and risk management determines a need.	
TOTAL THIS AREA / 6	

7.3.6.14 Configuration

Issue	*Rate*
Configurations are controlled for all systems.	
Configurations for non-low surety systems must pass change control.	
Configuration management systems must be at least medium surety.	
Separation of duties is maintained for configuration management.	
TOTAL THIS AREA / 4	

Copyright © 1977-2005 Fred Cohen & Associates – All Rights Reserved

7.3.6.15 Applications

Issue	*Rate*
Applications that require interaction across surety levels have protections for crossing surety boundaries.	
Risk management dictates protection requirements for applications crossing surety boundaries.	
Input and output controls enforce encryption requirements.	
Input and output controls enforce authentication requirements when appropriate.	
Input controls enforce length, syntax, and consistency requirements.	
State machine modeling and intrusion detection are used to validate input when risk management deems appropriate.	
Redundant sourcing is used when additional verification is appropriate to the integrity need.	
Access controls per the security architecture are implemented at the application layer as well as the OS level.	
TOTAL THIS AREA / 8	

7.3.6.16 Databases

Issue	*Rate*
Query limits are used on databases.	
Database access controls are used on databases.	
Databases provide audit records of all transactions.	
Transaction integrity is enabled in database systems.	
Redundancy is maintained for databases with non-low consequence.	
Separation of duties is enforced for non-low consequence databases.	
Data aggregation controls are used if risk management dictates it.	
Replay and rollback is available for non-low consequence databases.	
High consequence databases are maintained at redundant locations with all necessary components for disaster recovery.	
Access controls per the security architecture are implemented at the database layer.	
TOTAL THIS AREA / 10	

7.3.6.17 Storage Area Networks

Issue	*Rate*
Geographic and local redundancy are used for storage area networks (SANs) associated with medium or high valued information.	
Separation of duties for SAN operation and operation of systems accessing SANs is maintained for medium and high surety systems.	
Backup of SAN content is stored at geographically distant locations as specified by radius requirements of risk management.	
Risk management dictates the use of RAID for SAN storage.	
Communication to non-local SANs is encrypted and authenticated.	
TOTAL THIS AREA / 5	

7.3.6.18 Roll-up

Enter Rating from above. Rate business criticality and value from 1 to 10.

Issue	*Business Criticality*	*Business Value*	*C*V*	*Rating*	*C*V*R/10*
General					
Mainframes					
Midrange					
Servers					
Clients					
Firewalls					
Networks					
Telephony					
Backbone					
Cabling					
Hosts					
External links					
OS's					
Configuration					
Applications					
Databases					
SANs					
Totals					

Overall weighted rating = sum of (C*V*R/10) / sum of (C*V) =

Startup	***Diligence***	***Typical***	***Excellent***	***Best***
2	5	6	7	9.5

Copyright © 1977-2005 Fred Cohen & Associates – All Rights Reserved