9.2.3 Systems

Rate each item from 0 to 10 then sum the ratings to generate an overall rating.

9.2.3.1 Conception

Item	*Rate*
The protection concepts associated with systems are an integral part of their conception.	
Enter rating here	

9.2.3.2 Design

Item	*Rate*
Design integrates information protection issues as basic design goals and requirements.	
Designers consider all of the life cycle areas and requirements for integrity, availability, confidentiality, use control, and accountability.	
Designers have adequate expertise to make reasonably good design decisions with regard to protection issues.	
Design teams have adequate background and education in these specialty areas to be effective at protection design.	
Designs embrace integration into the enterprise protection architecture.	
Total all ratings and divide by 5	

9.2.3.3 Engineering

Item	*Rate*
Engineering practices embody protection practices.	
Engineering teams include individuals with extensive protection engineering experience.	
Engineering measures itself against the CMM-SEC criteria and achieves the enterprise-specified level of maturity.	
Total all ratings and divide by 3	

9.2.3.4 Implementation

Item	*Rate*
Implementation goes through a well-defined process that integrated protection issues at all levels.	
Procurement includes provisions for protection to prevent the introduction of Trojan horses into procured elements of high risk systems.	
Design and code reviews integrate security reviews.	
Protection testing and change control processes are integrated into implementation of all medium and high risk systems.	
Implementation integrates system audit with enterprise audit and enterprise control into system control.	
Integration of intrusion detection and response systems, identity management, zoning, and other protections into systems happens in implementation prior to acceptance.	
Total all ratings and divide by 6	

9.2.3.5 Operation

Item	*Rate*
Operation of systems involves all of the enterprise protection processes and produces meaningful metrics.	
Operation generates audit trails, acts properly on control signals, fails in a safe mode for the rest of its environment, and remains within control constraints at all times.	
Operation is at the surety level suitable to the risk levels of the systems and their content.	
Total all ratings and divide by 3	

9.2.3.6 Maintenance

Item	*Rate*
Maintenance processes have special protective modes and controls.	
Separation from other systems during maintenance is required for medium and high risk systems.	
Sound change control processes are mandatory for medium and high risk systems.	

Item	Rate
Verification and reintegration after maintenance is required for medium and high risk systems.	
Maintenance processes have separation of duties requirements and controls over their presence and access is maintained in medium and high risk systems.	
Storage media used in maintenance is protected as is data associated with testing processes.	
Special access and passwords associated with maintenance processes are only available during those processes for medium and high risk systems.	
Maintenance access is disabled in normal operation for non-low risk systems/	
Total all ratings and divide by 9	

9.2.3.7 Disasters

Item	Rate
Overall business function is able to survive all disasters that leave most of its potential business operating.	
Adequate redundancy is available for every critical business function outside of the maximum radius of effect of mitigated threats and consequences.	
Redundancy in capabilities and diversity of locations is adequate for the worst case planned disasters.	
In risk management terms, overall protection objectives are met even when physical disasters grant unusual physical access.	
A well-defined and properly operated disaster recovery program is in place, regularly tested, and effective.	
Total all ratings and divide by 5	

9.2.3.8 Recovery

Item	Rate
Recovery processes have the ability to restore business operations in a timely fashion after a disaster.	
Recovery includes people, systems, data, and business change-overs and is a well tested and practiced plan.	

Item	Rate
Recovery processes have well defined starting and ending conditions and process checks along the way.	
Risk management dictates that changes in risk profiles associated with recovery are either acceptable or otherwise mitigated as part of the recovery process.	
Total all ratings and divide by 4	

9.2.3.9 Upgrades

Item	Rate
For medium and high valued systems, change control processes are required for all upgrades.	
Testing covers operation over a period of time under benign and malicious circumstances.	
Malicious upgrades are mitigated by verifying the source and integrity of the upgrade as part of change control.	
Change control over systems changes that are not able to be done in a sound manner are based on formal risk acceptance.	
As the value of the system increases, acceptance of risks from upgrades is made harder and harder.	
Total all ratings and divide by 5	

9.2.3.10 Transformations

Item	Rate
Transformations of systems from function to function are planned to assure ongoing protection effectiveness.	
Enter rating here	

9.2.3.11 Consolidation

Item	Rate
Consolidation of systems to join functions only happens after risk management approves the aggregation of risks involved.	
Proper safeguards are taken to compensate for the change in risk and surety requirements.	
Total all ratings and divide by 2	

9.2.3.12 Obsolescence

Item	*Rate*
As systems enter obsolescence changes in utility of the system and its criticality result in a properly controlled reduction in risk and surety.	
Enter the rating here	

9.2.3.13 End-of-life

Item	*Rate*
As systems are decommissioned care is taken to assure that they are no longer needed.	
Systems are operated for at least one full business cycle of every critical function before shut down.	
Residual data confidentiality is protected by destruction or ongoing protection.	
After system shut down, audit trails and accountability requirements are met until all value is certified as gone.	
Formal processes are used for system end-of-life.	
Total all ratings and divide by 5	

9.2.3.14 Reconstitution

Item	*Rate*
Reconstitution of systems after the end of their life cycle must meet all of the protection requirements associated with system creation.	
Reviews for changes between shut down and reconstitution are required.	
After reconstitution, normal processes associated with end-of-life must be redone when the system is again decommissioned.	
Total all ratings and divide by 3	

9.2.3.15 Resale

Item	*Rate*
Resale of systems after decommissioning requires verification of the decommissioning process and residual data destruction and retention.	
Enter the rating from above	

9.2.3.16 Destruction

Item	*Rate*
Systems are destroyed when component junk value exceeds system resale value or when destruction is less expensive than secure alternatives.	
End of life processes assure that residual value is appropriate and destruction may proceed following all applicable laws and regulations associated with environmental and health standards.	
Parts with hazardous chemicals, such as PCBs, are handled so as to properly deal with downstream liability.	
Special processes are used for accidental or maliciously destroyed systems to assure that value of content and audits are retained and leakage is properly controlled.	
Total all ratings and divide by 4	

9.2.3.17 Recycling

Item	*Rate*
Recycling of components and materials takes into account risk management requirements.	
Enter the rating from above here	

9.2.3.18 Roll-up

Area	*Rate*
Conception	
Design	
Engineering	
Implementation	
Operation	
Maintenance	
Disasters	
Recovery	
Upgrades	
Transformations	
Consolidation	
Obsolescence	
End-of-life	
Reconstitution	
Resale	
Destruction	
Recycling	
Total ratings and divide by 17	

Startup	*Diligence*	*Typical*	*Excellent*	*Best*
1	7	7	8	10