7.3.9 Auditing

7.3.9.1 Internal

Item	*Rate*
Internal audit processes are used to assure that operations meet internal requirements on a day-to-day basis.	
Audit staff are sufficient and knowledgeable enough to carry out their audit duties with respect to security.	
High valued systems are audited more thoroughly and more often than medium valued systems.	
Medium valued systems are audited more often and more thoroughly than low valued systems.	
High valued systems are audited at least twice per year.	
Audit covers all aspects of the information protection program.	
Audit reports results to the CISO.	
Internal audit is treated as a collaborative process rather than an oppositional process.	
Audit cannot modify anything in any system they audit.	
Audit results are acted on promptly.	
Total this area / 10	

7.3.9.2 External

Item	*Rate*
External audit verifies that internal audit is doing its job properly.	
External audit verifies compliance with regulatory and other mandatory requirements.	
External audit reports results to the CISO along with others as appropriate.	
External audit cannot alter anything in systems they audit.	
External audit results are acted on promptly.	
Total this area / 5	

7.3.9.3 Period

Item	Rate
Periods for audits is determined by risks, costs, resources, time required.	
All high-risk systems are audited at least twice per year.	
All medium-risk systems are audited at least yearly.	
Random and surprise audits are undertaken against select systems.	
All CISO functions are audited at least once per year.	
Total this area / 5	

7.3.9.4 Standard

Item	Rate
Internal audit standards are agreed to by risk management, and CISO.	
Internal auditors rate against the identified standards.	
Standards change slowly so measurements over time are comparable.	
Internal audit attempts to model external audit.	
External and internal auditors must provide details of what standards they are auditing to long enough prior to the commencement of audits for the CISO to properly prepare for those audits.	
Total this area / 5	

7.3.9.5 Coverage

Item	Rate
Coverage levels for audits are defined by risk management.	
Coverage for high risk systems is no lower than for medium risk systems.	
Coverage for medium risk systems is no lower than for low risk systems.	
Coverage at the program level for the CISO function is 100%.	
Audits provide higher coverage for higher risk program components.	
Total this area / 5	

Sum these areas and divide by 5 for an overall rating

Internal	External	Period	Standard	Coverage	Rate

Startup	Diligence	Typical	Excellent	Best
2.5	5	6	7	9.5