Requirements and Testing Procedures		Guidance
Defined Approach Requirements	**Defined Approach Testing Procedures**	**Purpose** If roles and responsibilities are not formally assigned, networks and systems may not be properly protected from malware. **Good Practice** Roles and responsibilities may be documented within policies and procedures or maintained within separate documents. As part of communicating roles and responsibilities, entities can consider having personnel acknowledge their acceptance and understanding of their assigned roles and responsibilities. **Examples** A method to document roles and responsibilities is a responsibility assignment matrix that includes who is responsible, accountable, consulted, and informed (also called a RACI matrix).
5.1.2 Roles and responsibilities for performing activities in Requirement 5 are documented, assigned, and understood.	**5.1.2.a** Examine documentation to verify that descriptions of roles and responsibilities for performing activities in Requirement 5 are documented and assigned.	
	5.1.2.b Interview personnel with responsibility for performing activities in Requirement 5 to verify that roles and responsibilities are assigned as documented and are understood.	
Customized Approach Objective		
Day-to-day responsibilities for performing all the activities in Requirement 5 are allocated. Personnel are accountable for successful, continuous operation of these requirements.		
5.2 Malicious software (malware) is prevented, or detected and addressed.		
Defined Approach Requirements	**Defined Approach Testing Procedures**	**Purpose** There is a constant stream of attacks targeting newly discovered vulnerabilities in systems previously regarded as secure. Without an anti-malware solution that is updated regularly, new forms of malware can be used to attack systems, disable a network, or compromise data. **Good Practice** It is beneficial for entities to be aware of "zero-day" attacks (those that exploit a previously unknown vulnerability) and consider solutions that focus on behavioral characteristics and will alert and react to unexpected behavior. **Definitions** System components known to be affected by malware have active malware exploits available in the real world (not only theoretical exploits).
5.2.1 An anti-malware solution(s) is deployed on all system components, except for those system components identified in periodic evaluations per Requirement 5.2.3 that concludes the system components are not at risk from malware.	**5.2.1.a** Examine system components to verify that an anti-malware solution(s) is deployed on all system components, except for those determined to not be at risk from malware based on periodic evaluations per Requirement 5.2.3.	
	5.2.1.b For any system components without an anti-malware solution, examine the periodic evaluations to verify the component was evaluated and the evaluation concludes that the component is not at risk from malware.	
Customized Approach Objective		
Automated mechanisms are implemented to prevent systems from becoming an attack vector for malware.		