1. User and Access Management   
Control Assessment: Verify employment and need-based access to ensure appropriate user access workflows.  
  
Audit Focus: Examine the processes for allocating and terminating user accounts, especially for departing employees. Verify that the least privilege concept is being followed, and verify the accuracy of access control logs.  
  
2. Patch Management, Vulnerability Assessment, and Antivirus   
  
Control Assessment: AT&T employs procedures to assess system flaws and implement fixes to fix vulnerabilities.  
  
2. Vulnerability assessment, patch management, and antivirus  
control assessment: AT&T uses processes to assess system flaws and deploy patches to fix vulnerabilities.  
  
 Audit Focus: Verify that frequent vulnerability assessments are carried out, patching schedules are followed to, and antivirus signatures are up-to-date.

4. Endpoint Detection and Response (EDR)   
Control Assessment: EDR tools help to secure endpoints by monitoring and responding to threats on individual devices.  
  
Audit Focus: Examine how EDR software is installed on workstations, laptops, and mobile devices, among other endpoints. Make certain that threat detection data is regularly examined and addressed.  
  
5. SIEM Event Correlation  
Control Assessment: To identify threat patterns, Security Information and Event Management (SIEM) correlates security event data.  
  
Audit Focus: Verify that the SIEM system is set up appropriately and that events are successfully correlated across different security levels (network, endpoint, etc.). Examine incident logs to identify threat patterns in real time.

6. Incident Response

Control Assessment: AT&T has established a Security Incident Response process to investigate and address potential security attacks.

Audit Focus: Evaluate the incident response plan’s effectiveness, including response time and containment measures, and verify post-incident analysis for continuous improvement.

7. Security Operations Center (SNOC)

Control Assessment: SNOC monitors and responds to security events in real-time.

Audit Focus: Assess SNOC staffing, tools, and incident handling efficiency. Ensure procedures align with industry best practices and that the SNOC team regularly reviews and acts on security alerts.