The chart outlines assessment items which have been grouped topically. References to the specific requirements in the Outsourcing Standard for Non-Channelers and the *CJIS Security Policy* have also been provided for each assessment item. Depending on the function outsourced and the specifics of the process, all of the requirements listed may not be applicable.

Sample 90 day Audit Checklist for an Authorized Recipient

Contractor Assessment	Reference OS-Outsourcing Standard for Non-Channelers CSP-CJIS Security Policy	Yes	No	N/A
Policy References				
a. Copy of current Outsourcing Standard for Non-Channelers	OS 2.02, 2.03, 2.05, 2.07, 3.02, 3.03, 5.03, 6.02, 7.01, 8.01a, 9.01, 9.04, 11.05, 11.06			
b. Copy of current *CJIS Security Policy*	OS 2.03b, 2.03c, 3.01, 3.02, 3.03, 7.01, 7.02, 9.02			
Security Program				
a. Authorized Recipient (AR) approved minimum requirements for content of Security Program	OS 3.02			
b. Implementation of security requirements	OS 3.02, 3.03 a-d			
c. Reporting procedures for security violations	OS 3.03(c), 8.0			
Security Training Program				
a. AR approved	OS 3.04			
b. Training prior to appointment or assignment	OS 3.04			
c. Training upon receipt of changes	OS 3.04			
d. Annual refresher training	OS 3.04			
Site Security				
a. Available for announced/unannounced audits	OS 3.05			
b. Physically secure location	OS 4.01, 7.02a			
Use and Maintenance of CHRI				
a. Maintained in accordance with contract and does not exceed period of time AR is authorized to maintain	OS 3.07			
b. Used only in accordance with contract and AR's authority	OS 2.03, 3.01			
Dissemination				
a. AR approved in accordance with contract and AR's authority	OS 5.01			
b. Compliant with laws, rules, and regulations[1]	OS 5.01			
c. Log captured required information and retained for a minimum of 365 days	OS 3.08, 5.02			
Personnel Security				
a. Criminal background checks on all Contractor and approved sub-Contractor personnel with access to CHRI conducted prior to access	OS 6.01			
b. Confirmation of understanding by employee(s)	OS 6.02			
c. List of personnel with access to CHRI	OS 6.03			
d. Updates to list of personnel changes within 24 hours of changes	OS 6.03			

[1] Applicable laws, rules, and regulations regarding the dissemination of national CHRI include Title 28, United States Code, Section 534; Title 28, Code of Federal Regulations, Section 50.12 (b) and Part 906.

Contractor Assessment	Reference OS-Outsourcing Standard for Non-Channelers CSP-CJIS Security Policy	Yes	No	N/A
Security Violations				
a. Develop and maintain written security violation plan	OS 8.01a, 2.07, 3.03			
b. Policy for disciplinary action	OS 8.01a			
c. Immediate suspension pending investigation	OS 8.01b			
d. Immediate report	OS 8.01c			
d. Follow-up report	OS 8.01c			
Security on Systems Processing CHRI				
a. Current topological drawing	OS 2.04			
b. Firewalls	OS 7.01a, CSP 5.10			
c. Encryption	OS 7.01b, CSP 5.5.2.4, 5.10.1.2			
f. Virus protection on networks processing CHRI	CSP 5.10.4.2			
g. User identification	CSP 5.6			
h. Authentication of user identification	CSP 5.6			
i. Advanced authentication when accessing via the Internet	CSP 5.6			
j. Audit trails	CSP 5.4.6			
Media Destruction				
a. Hard copy	OS 7.02c, CSP 5.8.4			
b. Electronic media	OS 7.02, CSP 5.8.3			