- Verifica della presenza della firma del dirigente, del funzionario istruttore e del funzionario revisore sulla check list AGEA;

- Verifica corretta contabilizzazione;

In merito alle uscite di zucchero le verifiche effettuate sono state le seguenti:

ISTRUTTORIA:

- Verifica della completezza della documentazione per la richiesta del contributo:
  a. Bando di gara permanente della Commissione;
  b. Decisione della Commissione di fissazione del prezzo minimo da applicare per la rivendita dello zucchero
  c. Data
  d. Prezzo
- Offerta di acquisto:
  a. Dichiarazione dell'offerente
  b. Fidejussione in corso di validità
- Lettera di aggiudicazione
- Lettera di conferma ricevuta aggiudicazione
- Modello 121 T attestante il pagamento del prodotto acquistato
- Buono di ritiro
- Analisi della partita di zucchero oggetto di acquisto
- Verbale dell'ufficio tecnico in merito alla regolarità del controllo eseguito dal laboratorio analisi
- Fattura di vendita AGEA
- Verifiche relative alla conformità documentazione - normativa comunitaria/nazionale
  a. Verifica del rispetto del quantitativo minimo di offerta d'acquisto
  b. Verificare che la lettera di comunicazione-aggiudicazione venga inviata all'offerta più favorevole
  c. Verificare che la fidejussione sia stata presentata secondo quanto previsto dal bando di gara
  d. Verificare che il termine di ritiro del prodotto sia stato rispettato

RICALCOLO:

- Q.tà di zucchero venduta da Agea (in tonnellate)
- Prezzo unitario di acquisto
- Prezzo totale di acquisto
- Iva sull'acquisto (10%)
- Prezzo totale incassato
- Ricevuta Modello 121 T

- Eventuale delta
- Note PwC

ENTRATA:

- Verifica esattezza del versamento effettuato e risultante dal modello 121T B Italia

CORRETTA REGISTRAZIONE:

- Verifica ex finanziario
- Verifica capitolo italiano
- Verifica capitolo italiano per l'IVA

Dai test di dettaglio non sono emersi rilievi.

5.4 Valutazione della gestione del sistema informativo

Nell'eseguire l'incarico di revisione conferitoci per l'organismo pagatore AGEA per l'anno finanziario terminato il 15.10.2006, abbiamo considerato gli orientamenti interpretativi emanati in data 19 Novembre 2004 dalla Direzione generale agricoltura della Commissione europea con il documento AGRI-2004-60334-01-00-IT-TRA- 00 ed intesi a chiarire il punto 6.vi) dell'allegato al regolamento (CE) n°1663/95 del 7 Luglio 1995, così come modificato dal regolamento (CE) n° 465/2005 della Commissione del 22 marzo 2005 relativamente alla sicurezza dei sistemi d'informazione.

Come previsto dagli orientamenti stessi, a partire dall'esercizio finanziario 2008 l'organismo pagatore dovrà garantire la sicurezza del proprio sistema d'informazione sulla base dei criteri stabiliti in una versione, applicabile nel corso dell'esercizio finanziario considerato, di una delle seguenti norme internazionali riconosciute:

1) Organizzazione internazionale per la standardizzazione ISO 17799/ norma britannica 7799: Codice di buona pratica per la gestione della sicurezza delle informazioni (BS ISO/IEC 17799);
2) Bundesamt für Sicherheit in der Informationstechnik (Ufficio federale per la sicurezza delle tecniche dell'informazione): IT-Grundschutzhandbuch / IT manuale di sicurezza informatica di base (BSI);
3) Information Systems Audit and Control Foundation: Control Objectives for Information and related Technology – COBIT (obiettivi di controllo nel campo dell'informazione e delle tecnologie correlate).

Le misure di sicurezza devono essere adeguate alla struttura amministrativa, al personale e all'ambiente tecnologico di ogni organismo pagatore e l'impegno finanziario e tecnologico deve essere proporzionale ai rischi effettivi.

AGEA ha scelto di garantire la sicurezza del proprio sistema d'informazione sulla base dei criteri stabiliti della norma internazionalmente riconosciuta denominata ISO17799 (come richiamato al punto 1 di cui sopra).

In applicazione dell'orientamento previsto nel paragrafo 3.2) del richiamato documento, riportiamo di seguito:

1) una premessa necessaria all'inquadramento dell'organizzazione dell'organismo pagatore;

2) il dettaglio dei risultati delle osservazioni e conclusioni provvisorie comprensivo di raccomandazioni e punteggio di maturità per ogni dominio della norma espresso sulla base del modello previsto dal citato orientamento.

Le osservazioni e conclusioni sono state formulate sulla base delle interviste condotte con i responsabili dell'organismo pagatore e della comprensione avvenuta analizzando la documentazione fornitaci nel corso dell'intervento.

La sintesi delle raccomandazioni è riportata nel capitolo 1 classificata tra le risultanze.

5.4.1 Premessa

AGEA ha stipulato una contratto con il fornitore AGRISIAN per la gestione del proprio sistema informativo (SIAN).

L'outsourcer AGRISIAN è formato dalle seguenti sette società certificate ISO:
- Finsiel SpA;
- Sofiter SpA;
- Auselda AED Group SpA;
- IBM Italia SpA
- Telespazio SpA;
- Agrifuturo soc.coop a.r.l.;
- Cooprogetti s.c.r.l. Engineering Consulting.

L'intero sistema informativo (apparecchiature, sistemi, programmi, dati ecc.) oggetto di audit è dunque localizzato nelle strutture di AGRISIAN; l'Agenzia è comunque dotata di infrastruttura di office automation che governa direttamente.

Il contratto con AGRISIAN non si limita alla sola fornitura di software e hardware, ma alla completa assistenza su ogni tipo di problematica legata alle procedure automatizzate di gestione degli aiuti.

Il fornitore risponde completamente del servizio informativo compreso nell'ambiente informativo SIAN assicurando la produzione, la manutenzione e la gestione di tutte le procedure inerenti agli aiuti comunitari.

AGRISIAN è parte attiva anche nella definizione delle strategie e della pianificazione dell'ambiente dei Sistemi Informativi.

Il contratto in questione prevede che i servizi di natura informatica siano sottoposti a monitoraggio, nel rispetto e nei confini di applicabilità della circolare AIPA (ora CNIPA) CR/5 del 5.8.1994.

5.4.2 Modello di misurazione del grado di maturità

Il modello di misurazione del grado di maturità utilizzato è applicato ai domini della norma internazionale scelta ancorché le pratiche di controllo adottate siano esternalizzate. Il punteggio di conformità sotto espresso corrisponde al punteggio più basso per uno dei quattro aspetti del dominio esaminato (a-d) senza mediare i risultati.
Ogni categoria prende in esame, laddove applicabili, i seguenti aspetti/dimensioni sulla base dei quali è possibile misurare i domini della norma:

a)il riconoscimento e la comunicazione del problema,
b)la politica da seguire,
c) la formazione ed i processi associati per mettere in pratica la politica da seguire,
d) la misurazione dell'efficacia della politica e dei processi associati ed i miglioramenti ottenuti.

Il punteggio è espresso in forma sintetica secondo la scala riportata alla tabella seguente.

Punteggio di conformità	Livello di maturità associato al punteggio
0	Inesistente
1	Iniziale/Ad hoc
2	Ripetibile, ma intuitivo
3	Processo definito
4	Gestito e misurabile
5	Ottimizzato

Osservazioni e conclusioni provvisorie

Riportiamo i risultati, le raccomandazioni ed il punteggio di conformità per ciascun dominio della norma internazionale scelta validi per le applicazioni significative che supportano ciascuna delle tre funzioni dell'organismo pagatore (autorizzazione, pagamento e contabilizzazione).

5.4.3 Security Policy

Punteggio di conformità: 3

Risultato:
AGEA ha esternalizzato la gestione del proprio sistema informativo (SIAN) presso l'outsourcer AGRISIAN ed ha compreso la necessità di affrontare le tematiche connesse all'emanazione di un documento di Security Policy.

Tuttavia AGEA non ha emanato una propria security policy, ma è stato invece redatto il Documento Programmatico della Sicurezza (DPS) che fa riferimento alle policy emanate dall'outsourcer.

Raccomandazione:
Se pur presente un Documento Programmatico della Sicurezza, raccomandiamo all'Agenzia di approvare una specifica Policy di sicurezza la quale dovrebbe essere poi distribuita a tutte le parti interessate ed essere periodicamente rivista. Il documento dovrebbe almeno contenere:

1)una definizione della sicurezza informatica, i suoi obiettivi, il perimetro di validità;
2)un'affermazione di principio circa l'intento dell'alta direzione di allineare la policy con gli obiettivi dell'ente;
3)la definizione dell'utilizzo della metodologia di analisi dei rischi strumentale all'emanazione delle procedure di dettaglio;
4)la definizione delle responsabilità connesse all'implementazione della policy, etc...

5.4.4 Organization of Information Security

Punteggio di conformità: 3

La necessità di affrontare le problematiche connesse all'organizzazione della sicurezza sono comprese e accettate dall'Agenzia.

In generale ruoli e responsabilità sono definiti in linea con le politiche dell'organizzazione aziendale infatti, con apposite delibere (n° 169 e n°170), l'Agenzia ha definito:

- il ruolo del responsabile della sicurezza, a cui è demandata la responsabilità delle politiche di sicurezza AGEA, ma tale ruolo è vacante dal 15 agosto 2005;
- un comitato per la sicurezza ad alto livello formato da personale proveniente da diverse aree funzionali.

Gli aspetti connessi all'organizzazione della sicurezza, per la parte esternalizzata e relativa al sistema informativo SIAN, sono disciplinati nel contratto tra AGEA ed AGRISIAN del 2001 così come modificato nel 2003.

Tale contratto tuttavia non contempla esplicitamente clausole su come soddisfare gli adempimenti di legge, relativi alla normativa sulla protezione dei dati.

Raccomandazione:
Si dovrebbe valutare l'opportunità di nominare un Responsabile della Sicurezza di Agea, figura significativa per quanto riguarda l'organizzazione della sicurezza e la gestione delle politiche collegate.

Si dovrebbe inoltre prevedere che tutti i contratti stipulati da Agea con le terze parti contemplino esplicitamente clausole su come soddisfare gli adempimenti di legge, relativi alla normativa sulla protezione dei dati, in accordo con quanto previsto all'articolo 8 dal regolamento applicativo del Decreto legislativo 196/03 in materia di trattamento dei dati personali.

5.4.5 Asset Management

Punteggio di conformità: 2

All'interno dell'organizzazione si è coscienti dell'esistenza delle tematiche relative alla gestione degli asset.

A tal fine sono predisposte attività di inventariato e di censimento dell'Hardware e del software utilizzato.

E' stato emanato il Documento Programmatico della Sicurezza (DPS) che contiene una classificazione delle informazioni sotto il profilo della sensibilità e strumentale a garantire la conformità con la normativa nazionale in tema di privacy.

Le informazioni sono dunque state classificate come "non sensibili" ma le stesse non sono state contrassegnate in modo da evidenziare quelle maggiormente critiche per l'Agenzia e che necessitano di un maggiore livello di protezione.
In generale non tutte le informazioni sono classificate pertanto vengono gestite con lo stesso livello di sicurezza. Si precisa inoltre che per informazioni si intende non solo i dati residenti sui sistemi informativi ma tutte le tipologie di informazioni gestite dall'ente (ad esempio: manuali, contratti, materiale di training, documentazione etc.)

Raccomandazione:
E' auspicabile che l'Ente proceda alla classificazione delle informazioni non solo sotto il profilo della sensibilità, ma anche in base al loro valore, ai requisiti legali e criticità verso l'organizzazione.

In generale la non classificazione delle informazioni ostacola la possibilità di gestire in modo efficiente ed ottimale il sistema di controllo interno non palesando all'organizzazione il valore degli stessi.

Anche le informazioni che non necessitano di alcuna protezione (qualora presenti) dovrebbero essere formalmente individuate.

5.4.6 Human Resources Security

Punteggio di conformità: 2

All'interno dell'organizzazione si è coscienti dell'esistenza delle problematiche connesse alla protezione dei dati e dei sistemi da azioni umane intenzionali e/o accidentali.

Gli aspetti connessi alla gestione della sicurezza nella definizione e nella regolamentazione dei contratti di lavoro seguono i requisiti indicati nel CCNL (Contratto Collettivo Nazionale di Lavoro del Comparto Regioni e Autonomie Locali del 22/1/2004) e nel DPS emanato dall'organizzazione.

Gli accordi contrattuali con il fornitore AGRISIAN includono gli aspetti connessi alla responsabilità connesse alla sicurezza delle informazioni.

La dirigenza sensibilizza il personale agli aspetti connessi alla sicurezza logica e fisica dei dati, dei beni e delle informazioni.

E' prevista una sottoscrizione di un impegno di riservatezza per il personale (interno ed esterno) di AGEA a titolo di accettazione delle disposizioni in materia di sicurezza.

I diritti di accesso alle informazioni ed alle strutture di tutti i dipendenti interni/esterni di AGEA sono revocati al termine del rapporto di lavoro/contratto.

Raccomandazione:
La sezione della norma tratta le misure organizzative atte a mitigare i rischi connessi alla protezione dei dati da azioni intenzionali e/o accidentali da parte del personale.

In questo ambito si dovrebbe provvedere a:

- a documentare tra le mansioni del personale anche le responsabilità sulla sicurezza;
- a predisporre piani regolari di addestramento del personale per favorire comportamenti responsabili.

5.4.7 Physical and Environmental Security

Punteggio di conformità: 3

La necessità di affrontare il problema della sicurezza fisica ed ambientale è compresa e accettata dall'organizzazione.

La sicurezza fisica ed ambientale viene gestita tramite procedure coperte per la gran parte dall'outsourcer AGRISIAN°

Il CED presenta misure idonee a preservare i dati a fronte del verificarsi di eventi di natura accidentale quali:

- impianto anti-incendio
- rilevatori di fumo
- pavimento rialzato

- aria condizionata (20 gradi)
- gruppo di continuità
- generatore
- servizio di vigilanza (h24)
- video sorveglianza
- porte blindate (doppio riconoscimento)
- pavimento antivibrazioni

Le apparecchiature significative ed i locali aziendali sono gestiti secondo criteri di sicurezza.

5.4.8 Communications and Operations Management

Punteggio di conformità: 3

La necessità di affrontare il problema della gestione delle comunicazioni e dell'operatività è ben compresa dall'organizzazione.

Gli aspetti connessi alle modifiche del sistema informativo sono affidate all'outsourcer AGRISIAN le cui responsabilità sono definite all'interno di un contratto che prevede specifici livelli di servizio (SLA)
Il monitoraggio e la review dei servizi delle terze parti è effettuata attraverso le seguenti entità:

- il monitore (BAIN&Co) per il monitoraggio dei servizi disciplinati nel contratto AGEA-AGRISIAN
- Commissione di Verifica e Collaudo per il monitoraggio degli SLA
- Servizio di Controllo Interno

Esistono procedure per la definizione di responsabilità operative, per il funzionamento, lo sviluppo e la manutenzione dei sistemi e per il dimensionamento delle risorse.

Esiste separazione fisica e logica degli ambienti di sviluppo, test e produzione.

Sono presenti procedure di anti-virus e di back-up dei dati e del software.

Sono presenti procedure relative all'utilizzo della posta elettronica. Tali procedure tuttavia non contemplano:

- la conservazione dei messaggi che potrebbero essere utili in caso di vertenze legali

- una documentata valutazione dei rischi connessi all'utilizzo della posta elettronica.

Sono previsti log di sistema contenti informazioni significative dal punto di vista della sicurezza i quali sono rivisti periodicamente.

Raccomandazione:
Si dovrebbe valutare l'opportunità di estendere le procedure esistenti in materia di posta elettronica al fine di disciplinare gli aspetti connessi alla conservazione dei messaggi che potrebbero essere utili in caso di vertenze legali.

Dovrebbe inoltre essere effettuata una mappatura ed una valutazione formalmente approvata e documentata dei rischi connessi all'utilizzo della posta elettronica.

In considerazione dell'estrema ampiezza degli aspetti trattati in questo dominio è auspicabile una valutazione integrata degli stessi per migliorare l'implementazione di alcuni controlli tra cui quanto previsto dalla norma in materia di gestione dei media e dei supporti rimovibili e dell'audit logging.

5.4.9 Access Control

Punteggio di conformità: 2

All'interno dell'organizzazione si è coscienti dell'esistenza delle problematiche connesse al sistema di controllo degli accessi.

Sono presenti procedure volte a disciplinare le fasi del processo di creazione/modifica/eliminazione dei profili utente.
Tale processo contempla il rispetto dei principi di segregazione delle funzioni e di coerenza profilo attibuito-mansioni ricoperte, tuttavia non è presente un controllo di monitoraggio periodico (semestrale o annuale) dei profili.

E' stata emessa una procedura per l'utilizzo delle postazioni di lavoro (PDL) che prevede istruzioni per la protezione fisica e logica delle stesse. Tale procedura tuttavia non contempla gli aspetti connessi ai backup ed all'utilizzo di tecniche crittografiche delle PDL.

Non sono inoltre presenti policy e procedure di clear desk e clear screen°

Sono presenti sistemi di firewalling e di intrusion detection systems (IDS) a protezione della rete aziendale.

Sono state effettuate attività di penetration test.

La password policy del SIAN presenta caratteristiche di robustezza (scadenza automatica, lunghezza minima, numero massimo di tentativi di accesso, etc).

La procedura di logon non mostra dopo il completamento della stessa la data e l'ora del precedente logon positivo e i dettagli di ogni tentativo infruttuoso di logon°

Raccomandazione:
Si dovrebbe valutare l'opportunità di effettuare, con periodicità almeno semestrale, una revisione massiva di tutti i profili definiti sulle applicazioni oggetto di audit al fine di raggiungere obiettivi di segregazione dei compiti e di coerenza profili/status dipendenti.

Dovrebbe inoltre essere emanata una specifica policy e procedura di clear desk e clear screen°

Si dovrebbe valutare l'opportunità di estendere le procedure esistenti in materia di gestione delle postazioni di lavoro al fine di disciplinare, tra l'altro, gli aspetti connessi al backup ed alle tecniche crittografiche.

La procedura di logon sugli applicativi dovrebbe mostrare dopo il completamento della stessa la data e l'ora del precedente logon positivo ed i dettagli di ogni tentativo infruttuoso di logon al fine di fornire all'utente maggiore tracciabilità circa l'utilizzo della sua user ID.

5.4.10 Information Systems Acquisition, Development and Maintenance

Punteggio di conformità: 2

All'interno dell'organizzazione si è coscienti degli aspetti connessi all'acquisizione, allo sviluppo ed alla manutenzione dei sistemi e dei rischi connessi.

Una significativa parte del processo di sviluppo e manutenzione è affidato all'outsourcer AGRISIAN le cui responsabilità sono definite all'interno di un contratto che prevede specifici livelli di servizio.

Esistono procedure standardizzate e documentate per quanto riguarda la gestione degli interventi di modifica e gli sviluppi ai sistemi ed alle applicazioni oggetto di analisi (SIAN).

Tali procedure sono definite, condivise ed attuate dal fornitore.

AGRISIAN utilizza un software di Change Management (PVCS) al fine di registrare e misurare le performance connesse alle attività di gestione degli interventi di manutenzione/sviluppo sui sistemi informatici.

Sono presenti meccanismi crittografici, ma il loro utilizzo è limitato alle fasi di autenticazione e log on degli utenti.

Non sono dunque utilizzati meccanismi di cifratura delle informazioni. Queste soluzioni vengono applicate, per scelta di AGEA, solo sul settore vitivinicolo.

La trasmissione dati avviene su rete VPN dedicata da Telecom mentre i servizi acceduti dagli utenti sono su internet.

Raccomandazione:
Si dovrebbe valutare l'opportunità di implementare una policy sull'utilizzo dei controlli crittografici che contempli anche l'utilizzo e la gestione delle chiavi crittografiche.

5.4.11 Information Security Incident Management

Punteggio di conformità: 2

All'interno dell'organizzazione si è coscienti dell'esistenza delle problematiche connesse alla gestione degli incidenti legati alla sicurezza.

E' infatti disponibile un call center e un servizio di posta elettronica al fine di reperire informazioni dagli utenti circa eventuali vulnerabilità delle applicazioni maggiormente significative per AGEA.

AGEA si avvale delle procedure di incident management previste dall' SPC-CNIPA. Tuttavia non è prevista una procedura aziendale specifica in tema di classificazione e valutazione degli incidenti inerenti la sicurezza rivolta a tutti i dipendenti.

Raccomandazione:
Si dovrebbe valutare l'opportunità di emanare procedure specifiche e rigorose per la valutazione e la classificazione degli incidenti inerenti la sicurezza.

Tale procedure sono infatti strumentali per l'attuazione di un processo di analisi approfondita di tutte le tipologie di anomalie e deviazioni eventualmente verificabili e per supportare il management nella gestione tempestiva delle problematiche connesse a tali aspetti.

Tali procedure dovrebbero essere comunicate ed essere disponibili a tutti i dipendenti.

5.4.12 Business Continuity Management

Punteggio di conformità: 1

L'organizzazione ha riconosciuto l'esistenza del problema della Business Continuity e la necessità di mitigare i rischi di continuità.

Tuttavia, pur essendo presente un Disaster Recovery Plan per il SIAN, il Piano di Business Continuity è attualmente solo in stato di proposta da parte del fornitore AGRISIAN°

In caso di evento disastroso che coinvolga non solo i sistemi informativi della società il management potrebbe affrontare le problematiche derivanti da tale evento in maniera non preventiva e solo caso per caso, con misure ad hoc, senza un approccio trasversale comune.

Raccomandazione:
Raccomandiamo di finalizzare il piano di Business Continuity al fine di garantire la completa continuità aziendale anche in caso di eventi catastrofici: il piano dovrebbe essere testato ed aggiornato regolarmente.

5.4.13 Compliance

Punteggio di conformità: 1

Risultato:
All'interno dell'organizzazione si è coscienti dell'esistenza delle problematiche connesse alla conformità legale dei dati, del software, dei processi e del personale addetto.

Tali aspetti sono gestiti in modo implicito attraverso il coinvolgimento del fornitore AGRISIAN, delle strutture legali e della funzione Servizio di Controllo Interno. All'interno di quest'ultima funzione tuttavia risulta vacante il ruolo di IT Auditor.

Gli utenti sono stati sensibilizzati all'utilizzo del solo software licenziato ed i loro permessi non consentono di effettuare azioni di amministrazione della propria postazione di lavoro.

Non sono previste tuttavia livello di postazioni di lavoro, specifiche procedure (in particolare di natura automatica e preventiva) volte a massimizzare la coerenza tra numero di utenti, software utilizzati e relative licenze.

Raccomandazione:
Si dovrebbe valutare l'opportunità di estendere il sistema di controllo attualmente in essere prevedendo specifiche procedure per mitigare i rischi di non rispetto dei requisiti di conformità e con il copyright del software installato nelle postazioni di lavoro degli utenti Agea.

L'identificazione dei requisiti legali, regolamentari e contrattuali di conformità dovrebbe essere esplicito e non implicito e le procedure aziendali dovrebbero prevedere i controlli rilevanti alla mitigazione del rischio specifico.

CAPITOLO VI

6 ESAME DI CONFORMITA' CON I CRITERI PER IL RICONOSCIMENTO

La presente sezione descrive la situazione della conformità di Agea con i criteri di riconoscimento illustrati nell'allegato al Reg. CE n° 1663/95.

6.1 Situazione

Ai sensi del regolamento (CEE) n° 729/70 del Consiglio e successive modifiche e del regolamento (CE) n° 1663/95 della Commissione, ciascuno Stato membro deve provvedere al riconoscimento di uno o più organismi pagatori autorizzati ad erogare somme prelevate dai fondi FEAOG per conto della Commissione europea.
Per poter beneficiare del pieno riconoscimento, ciascun organismo pagatore deve soddisfare i criteri riguardanti le seguenti tre funzioni chiave:

- l'autorizzazione dei pagamenti;
- l'esecuzione dei pagamenti;
- la contabilizzazione dei pagamenti.

6.2 Procedure di riconoscimento per l'organismo pagatore

Abbiamo proceduto alla verifica dei criteri di riconoscimento stabiliti nell'allegato al regolamento (CE) n°1663/95.

Al fine di consentire una visione immediata della rispondenza dell'AGEA ai requisiti richiesti dal Reg. N°1663/95 per il riconoscimento come organismo pagatore (di seguito "OP"), di seguito riportiamo in modo schematico, l'elenco dei principali criteri di importanza rilevante con riferimento al punto 6 dell'allegato al regolamento sopra menzionato con le relative osservazioni.

Requisito/Punto dell'allegato al Reg. CE 1663/95	**Commento**
1. Atto formale che stabilisce i poteri	*L'Agenzia per le Erogazioni in Agricoltura* (AGEA), è un ente di diritto pubblico non economico, istituito con decreto legislativo 27 maggio 1999, n°165 e successive modificazioni e integrazioni.
2. Svolgimento delle tre funzioni in relazione alle spese FEAOG "garanzia"	L'AGEA nell'ambito dell'attività di organismo pagatore svolge le seguenti funzioni: - Autorizzazione dei pagamenti; - Esecuzione dei pagamenti; - Contabilizzazione dei pagamenti Per maggiori approfondimenti si rimanda a quanto esposto nel capitolo 4, paragrafo 4.4.
3. i) Istituzione del servizio di controllo interno	Con DM del 30 maggio 1996 è stato istituito un ufficio di revisione interna, la cui operatività è iniziata a partire dal 1997. Per maggiori approfondimenti rimandiamo a quanto esposto nel paragrafo 4.8
3. ii) Istituzione del servizio tecnico	Il servizio tecnico è stato istituito con D.M del 30 maggio 1996 (si veda quanto esposto nel paragrafo 4.7). La verifica degli elementi che giustificano i pagamenti ai beneficiari, i controlli in loco e altre verifiche tecniche sono svolte per la maggior parte dei casi avvalendosi della collaborazione di organismi delegati. I Regolamenti Comunitari prevedono, ad esempio, che per le misure relative allo Sviluppo Rurale ed alla Ristrutturazione Vigneti, la funzione di autorizzazione dei pagamenti sia completamente delegata alle Regioni in virtù dei piani regionali approvati dalla Commissione: in questi casi, l'Agea non ha alcun reale potere di controllo né di organizzazione (limitatamente alle Regioni), e la sua funzione è limitata alla emissione degli ordini di pagamento.
4. Delega delle funzioni	La delega delle funzioni è prevista dal Reg. CE 1663/95 Allegato articolo 4 e dalla linea direttrice 9. Ai sensi del Regolamento Comunitario e della linea direttrice 9 AGEA ha stabilito delle convenzioni con gli Organismi Delegati.