Ogni capo progetto è responsabile della messa in produzione di una applicazione.
Tutte le variazioni apportate ai programmi sorgenti vengono registrate in una rubrica ad hoc al fine di garantire un audit trail e la trasparenza delle operazioni.
Tutte le procedure operative sono documentate all'interno del manuale delle operazioni; l'attività di training e di formalizzazione è fatta in maniera capillare e tempestiva.

Le definizioni ed i parametri di controllo sull'attività produttiva sono custoditi in una libreria protetta e qualsiasi transazione al riguardo viene registrata e controllata.

I livelli di servizio sono definiti nel contratto, e sono previste sanzioni penali a carico di Agrisian, nel caso di mancato rispetto degli stessi.
Le attività relative ai processi di pagamento vengono controllate ed espletate in base a liste di controllo prestabilite.

Tutte le attività legate ad operazioni di elaborazione vengono registrate; una traccia viene conservata a scopo di revisione ed intervento.

5.4.8.5 Rapporti con fornitori/consulenti informatici

I rapporti con le società fornitrici di hardware, software e servizi sono gestiti direttamente dai responsabili delle aree e dal responsabile S.I. di AGRISIAN.
Ogni singolo acquisto è regolato da precise norme che prevedono di richiedere presso i maggiori fornitori i preventivi tecnici e di spesa con successiva gara.
Dall'analisi della migliore offerta tecnica e successivamente di quella economica viene individuato il fornitore che deve essere incaricato della fornitura.

5.4.8.6 Licenze Software

Esiste una normativa interna limitatamente ad AGRISIAN che disciplina l'uso del software. Non è consentita l'installazione di software che non sia quello di base fornito insieme al computer. Di fatto non esistono strumenti automatici di controllo per verificare l'utilizzo di software non autorizzato né licenziato.
L'inventario delle licenze viene gestito centralmente da Agrisian.

Agea ed Agrisian hanno adottato una procedura di gestione in sicurezza delle stazioni di lavoro assegnate agli utenti che ribadisce la responsabilità del dipendente nel corretto uso dello strumento di lavoro fornito dall'Organismo Pagatore, anche in conformità con quanto previsto dalle norme che disciplinano i rapporti di lavoro in materia di responsabilità e di riservatezza.

5.4.9 Criticità riscontrate per l'area "Sistemi di elaborazione e trasmissione dati"

Nel corso della nostra analisi che ha interessato l'area relativa ai "Sistemi di elaborazione e trasmissione dati/Applicazioni/Sviluppo e Manutenzione "Sviluppare e Acquisire le soluzioni dei Sistemi Informativi", che possiamo collocare nel dominio di Sviluppo e Acquisizione del SI di COBIT, abbiamo riscontrato alcune osservazioni che ci sembra rilevante riportare di seguito:

1. Molte esigenze utente sono soddisfatte autonomamente senza l'ausilio della direzione IT. Si riscontra la presenza di applicativi stand alone non adeguatamente presidiati dal fornitore. Questo perché attualmente nell'Agenzia sono presenti delle risorse che in passato sono state assunte per essere dedicate ai servizi IT, ma che, di fatto, attualmente non svolgono questa mansione. Tali risorse in passato hanno sviluppato degli applicativi stand alone che sono ancora in essere. Queste stesse risorse intervengono in modo informale, in caso di problemi sugli stessi applicativi stand alone. (Il fornitore non risponde, contrattualmente, degli applicativi che risiedono al di fuori del CED). Le applicazioni in questione hanno una significatività residuale, anche in quanto è stato pianificato un progressivo passaggio sui sistemi centrali.
2. Per il portale i controlli relativi all'efficienza e alle performance sono affidati ad IBM (fornitore del servizio).

Si rileva altresì che in seguito alla gara, relativa al bando pubblicato in data 31 ottobre 2003, che aveva per oggetto la fornitura di un servizio di monitoraggio del livello di servizio offerto da AGRISIAN, tale servizio è stato aggiudicato alla Bain & Co.
L'attività di monitoraggio è intesa a massimizzare il grado di conseguimento delle
finalità del contratto, e consiste in un sistema di operazioni di controllo riguardanti l'intero ciclo di vita di un sistema informativo automatizzato, con particolare riferimento:

- alla congruità del progetto con le linee strategiche del piano triennale;
- alla validità dello studio di fattibilità;
- alla corrispondenza dei prodotti/servizi progettuali con l'offerta tecnica;
- al rispetto degli obblighi contrattuali e di quanto enunciato nel capitolato di gara;
- alla verifica della opportunità di varianti;
- all'efficacia e l'efficienza della soluzione realizzata in relazione alle aspettative implicite ed esplicite dell'Amministrazione committente.

Alla data delle nostre verifiche risulta che la gara è stata aggiudicata, è stato stipulato il relativo contratto, l'attività di monitoraggio è in corso d'opera, ma non sono ancora disponibili i risultati delle analisi del monitore.

5.4.10 Il sistema di sicurezza fisica e logica

5.4.10.1 Sicurezza degli impianti ausiliari

Il CED, ubicato in un edificio gestito da IBM, è equipaggiato con contromisure necessarie alla protezione contro calamità fisiche (fuoco, accesso non autorizzato ed interruzioni di corrente).
L'accesso all'edificio dove è situato il Ced è presidiato 24 H da un servizio di guardania. Il guardiano ha a disposizione un elenco di persone autorizzate ad accedere all'edificio dopo le ore 22.00. L'accesso al CED è riservato al solo personale autorizzato, ed avviene tramite l'utilizzo di tesserini elettronici che consentono l'apertura della porta.
L'accesso di personale non autorizzato, o esterno, è possibile solo tramite l'accompagnamento di una persona addetta, e soltanto dopo l'apposizione di una firma in un apposito registro.
E' operativo un gruppo di continuità che assicura la fornitura di energia elettrica per la prevenzione di eventuali Black out.
Il CED è munito di dispositivi di allarme con rivelatori d'incendio. L'area è inoltre fornita di estintori antincendio. In caso di localizzazione di un incendio viene attivato un sistema con emissione di gas. All'interno della sala CED, è presente un sistema di monitoraggio della temperatura.
Le apparecchiature relative alla sicurezza fisica vengono revisionate con cadenza annuale in corrispondenza del rilascio delle procedure sulla sicurezza fisica.

5.4.10.2 Sicurezza delle linee di trasmissione dati

La rete locale su cui si basa la sede di via Palestro (Roma) è strutturata su 3 livelli di accesso:

- L'accesso all'interno è gestito da un unico firewall di collegamento, una stazione alfa con sistema operativo Unix con Altavista Firewall come software di limitazione accessi, la macchina è ad alta affidabilità con amplie ridondanze, che costituisce la prima barriera ed il primo punto di smistamento dei pacchetti a seconda dei protocolli usati.
- Successivamente a questa zona vi sono i sistemi web (che non sono ancora mission critical), la macchine applicative e le postazioni di lavoro
- Esiste poi un altro firewall identico al precedente come struttura per accedere ai data server.
- Il centro è dotato di sistemi di Intrusion Detection sia per quanto riguarda l'esterno che l'integrità dei dati all'interno, questi sistemi registrano dei possibili segnali di attacco dall'esterno, es. il port scanning, e automaticamente seguendo una procedura di escalation a seconda della gravità dell'attacco inviano messaggi e-mail ai membri della sicurezza o addirittura SMS sui cellulari in modo tale da permettere una reazione immediata.

5.4.10.3 Sicurezza di supporti magnetici di backup e dei documenti cartacei originali

I back-up di file di dati, i software applicativi e di sistema, la documentazione e le istruzioni operative vengono utilizzati con regolarità (quotidianamente o più spesso, se necessario), mediante una programmazione prefissata. Le copie di back-up vengono riposti ogni giorno in un luogo diverso dal centro di attività al fine di consentire un recupero in caso di incidente. Si precisa che le procedure prevedono la conservazione sia di copie On site che Off side.
Il funzionario operatore della AGRISIAN pianifica e scadenza sia i back-up che la conservazione dei dati, oltre alla cancellazione e al resettaggio degli strumenti quando tale conservazione non si rende più necessaria.
Per il Back-up scheduling viene applicata la seguente programmazione:

Sistemi di Produzione

- Backup full "OFF line" settimanali, tenuti per un mese (n.4 copie) ed effettuati di domenica;
- Backup Full "On line" giornalieri tenuti per 7 giorni: Backup Archive Log giornalieri, tenuti per un mese.

- Backup Export compressi giornalieri, tenuti per un anno.

Sistemi di collaudo

Non è previsto un backup dei dati, in quanto essi lavorano su copie ricavabili dai dati di produzione.

Sistemi di test

- Backup full "offline" (a DB spento) settimanali, tenuti per n.2 settimane (2 copie).
- Backup export compressi giornalieri, tenuti un massimo di 2 settimane.

5.4.10.4 Piano di disaster - recovery

In AGEA è documentato un piano di Disaster Recovery. Il piano è predisposto solo per gli applicativi batch.
I nastri di back up sono conservati settimanalmente in armadi ignifughi.
È effettuata una doppia copia dei nastri, una viene portata in un sito alternativo di sicurezza, come previsto dal piano di Disaster Recovery.
Questi sono conservati nei due siti alternativi (Perugia e Milano) come previsto dal piano di Disaster Recovery
È presente, presso il fornitore, un apparato UPS con autonomia di 45 minuti.

5.4.10.5 Controllo logico degli accessi alle risorse al S.I.

Accessi al software di sistema

Ambiente UNIX/ORACLE

L'accesso ai file di sistema è garantita dalle abilitazioni del sistema operativo stesso. Solo i sistemisti con i privilegi riservati assimilabili alla ROOT possono accedervi con il massimo livello di abilitazione.
Gli accessi alla root seguono la seguente prassi: ogni qual volta viene richiesto di entrare nel sistema con il privilegio di root la password viene consegnata all'utente in busta chiusa e immediatamente dopo la fine dell'utilizzazione viene cambiata.

Accessi al software applicativo.

L'accesso ai programmi del software di sistema è riservato esclusivamente alle persone autorizzate.
Il software TIVOLI (IBM) è stato installato per monitorare lo status della configurazione di sistema al fine di essere in regola con gli standard di sicurezza.

Una procedura automatizzata è in essere per informare (via e-mail ed sms) le persone interessate in caso di incidente, di attacco o di malfunzionamento del sistema. L'accesso ai dati è consentito in via interattiva mediante transazioni TP o attraverso procedure batch.
Ciascun utente, per accedere al sistema, ha bisogno di inserire una ID ed una password e può espletare soltanto i compiti che gli sono stati assegnati con il profilo ID.
Le ID, le password ed i profili vengono assegnati mediante l'applicazione di una procedura specifica denominata "Gestione Accessi".
La struttura organizzativa all'interno della AGRISIAN è conforme alla normativa 1663/95 che sancisce la "separazione degli incarichi" fra utenti finali, operatori e programmatori, oltre alla funzione specifica di "esecuzione dei pagamenti".
AGEA ha designato l'Ufficio Tecnico a gestire i rapporti con la AGRISIAN, al fine di raccogliere e trasmettere le richieste relative alla conservazione e alla creazione dei profili utente.
Lo schema generale della procedura prevede che i servizi informatici siano di proprietà di un Responsabile dei Servizi (solitamente un alto funzionario dell'Amministrazione) e che quindi l'utilizzo dei servizi debba essere autorizzato dal Responsabile dei Servizi.
La procedura in vigore per ottenere una User ID ed una Password è la seguente:

- l'utente deve compilare un modulo di richiesta, firmarlo e consegnarlo al funzionario di accesso all'utenza;
- l'ufficio gestione utenze esamina il modulo di richiesta e designa un dirigente dell'Agenzia di Erogazione in qualità di "responsabile AGEA", il quale potrà autorizzare la AGRISIAN a garantire l'accesso a questo nuovo utente;
- l'ufficio gestione utenze definisce il tipo di accesso da garantire ed invia il modulo all'impiegato responsabile interno all'AGEA;
- l'impiegato responsabile interno all'AGEA firma il modulo ed autorizza la AGRISIAN a rilasciare la User ID con le autorizzazioni elencate nel modulo stesso;
- l'ufficio gestione utenze impianta il profilo utente e assegna la password (che sarà disabilitata subito dopo la prima firma);

- l'ufficio gestione utenze invia, per posta ordinaria, la User ID e la Password inserendole in due buste differenti, mentre un documento viene inviato all'impiegato responsabile interno all'AGEA;
- l'impiegato responsabile interno all'AGEA firma il documento e prende le buste in cui sono contenute la User ID e la Password; queste vengono mantenute sigillate ed inviate all'utente finale.

Al fine di mantenere un adeguato livello di sicurezza logica, la AGRISIAN ha dotato il Sian di una protezione contro gli accessi illeciti. Il sistema di IDS (intrusion detection) è operativo e presidiato continuamente (H/24).

Sono presenti 2 Firewall a due livelli (CHECKPOINT), che comprendono una serie di politiche di sicurezza per:

- garantire e controllare l'accesso dell'utenza a servizi applicativi mediante un esclusivo punto di accesso protetto e controllato;
- garantire e controllare l'integrità del sistema, in caso di attacco dall'esterno;
- garantire l'implementazione del ruolo svolto dalla sicurezza sia per gli utenti interni che per quelli esterni (la AGRISIAN autorizza i propri impiegati ed esternamente autorizza gli utenti esterni (con accesso in sola lettura).

Il sistema di controllo accessi è gestito dal FIREWALL che agisce sulle abilitazioni per utente a vari livelli. L'identificazione e autenticazione dell'utente è attivata tramite immissione di User e Password, prevedendo per alcune aree il riconoscimento del terminale, tramite l'indirizzo IP ad esso collegato, da cui parte la transazione.

La lista delle User e livelli di abilitazione è gestita dai responsabili di gestione su richiesta della direzione organizzativa dell'AGEA.
La password per l'accesso al mondo Unix, che avviene tramite telnet, è robusta, di almeno 8 caratteri, cambiata ogni 28 giorni; il cambio della password, oltre ad essere automatizzato al momento del primo ingresso di un nuovo utente nel sistema, è automatizzato anche dopo la scadenza dei 28 giorni.

Accessi ai dati.

L'accesso ai file di dati mediante applicazioni di sistema richiede la preparazione di una richiesta formalmente firmata, che necessita di essere inoltrata dal supervisore diretto, per poi venire approvata dal responsabile del settore informatico.

Qualsiasi variazione effettuata ai dati viene registrata ed il funzionario alla sicurezza ne conserva traccia. Soltanto i programmi autorizzati e testati sono ammessi ai dati di produzione.
A ciascun utente viene richiesto di cambiare la propria password con cadenza trimestrale.
Le caratteristiche della password devono rispondere ai seguenti standard:

- Lunghezza minima (8 caratteri);
- Periodo di scadenza di 3 mesi;
- Il terminale si blocca automaticamente dopo cinque tentativi di firma a vuoto;
- I programmatori hanno una User ID per accedere esclusivamente all'ambiente test e sviluppo.

Infine, gli archivi dei dati possono essere modificati soltanto da transazioni specifiche o dai programmi batch.
L'agenzia effettua, inoltre delle verifiche periodiche (mensili) sulla sicurezza del sistema (penetration test).
In passato sono state svolte delle analisi dei rischi interni all'Agenzia da cui sono emerse le attuali policy adottate. Sono utilizzati strumenti di Intrusion Detection System (IDS).

5.4.11 Telecomunicazioni

La rete del Data Center del SIAN è organizzata in tre aree, interna, intermedia ed esterna ed è basata su di una infrastruttura LAN ad alta velocità ed elevata affidabilità.

All'area interna è assicurato il massimo livello di protezione; in essa sono presenti tutti i dati di produzione, le applicazioni di produzione tradizionale (TP e relativi sottogruppi) ed i sistemi di controllo di sicurezza.

All'area intermedia viene invece applicato un livello di protezione medio-alto; in essa sono presenti i sistemi con le relative tecnologie Internet/Intranet, ed include anche altri sistemi che consentono la fornitura di dati produttivi attraverso FTP.

Sull'area esterna sono infine attestati i collegamenti con le sedi centrali dell'Amministrazione e gli altri uffici periferici, nonché il collegamento alla rete internet utilizzato per veicolare l'acceso da parte dell'utenza ai servizi del portale del SIAN.

Presso ciascuna delle sedi centrali di AGEA è presente una rete LAN, utilizzata per il collegamento delle postazioni di lavoro ivi ubicate, oltre ai collegamenti su rete MAN, utilizzati per collegare le sedi centrali dell'Amministrazione con il Data Center del SIAN.

La rete del Data Center del SIAN e quella delle sedi centrali di AGEA di fatto realizzano una unica rete privata di tipo virtuale.

L'accesso alle tre aree è disciplinato dalle regole di sicurezza implementate su appositi apparati. In particolare sono presenti ed operativi tutti gli strumenti per la gestione ed il controllo delle politiche di indirizzamento e della sicurezza (firewall, router), nonché per la tracciatura e la documentazione del traffico. In particolare specifici apparati firewall sono posizionati a protezione degli accessi provenienti dalla rete pubblica Internet; in questo modo, anche nella eventualità di un evento "ostile" è possibile "chiudere" lo specifico collegamento, garantendo comunque continuità di servizio agli utenti istituzionali del SIAN.

Vengono infine adottati idonei accorgimenti contro l'introduzione di codici dolosi (per esempio i virus). Tutti i software ed i dati vengono controllati in relazione alla presenza di eventuali virus prima di essere caricati sui sistemi di elaborazione.

Attraverso specifici prodotti viene continuamente monitorato lo stato delle componenti di rete, rilevandone eventuali interruzioni delle funzionalità; in tal caso, i moduli a corredo, associati agli eventi di caduta e risalita delle componenti, provvedono ad inviare un messaggio e-mail al personale operativo e contemporaneamente registrano in un file di log gli eventi di interesse. Per le componenti di rete vengono anche raccolte informazioni statistiche e di prestazione al fine di consentire l'erogazione di un servizio proattivo alla risoluzione di eventuali criticità.

Altri prodotti sono deputati alla verifica della vulnerabilità dei sistemi e della rete, realizzando simulazioni di attacco e/o penetrazione con l'ausilio di programmi specifici (ISS/IDS). In tal modo è possibile valutare i rischi a cui è esposto il sistema informativo, attraverso l'analisi dell'impatto delle vulnerabilità segnalate (allarmi), e successivamente di individuare ed applicare le azioni più efficaci per il loro contrasto.
Alla data delle nostre verifiche abbiamo ottenuto i risultati del penetration test, effettuato dalla Bain & Co. da cui risulta che il sistema è complessivamente robusto.

La rete ed i software di comunicazione, con le relative variazioni, vengono verificati in conformità con i piani di controllo definiti dal piano di sicurezza generale (versione revisionata del 2005).

Linee ed apparati (router, switch), sono di proprietà amministrativa AGEA, mentre la definizione delle politiche di configurazione è gestita da AGRISIAN.

5.4.12 Operazioni di routine

Manutenzione dell'attrezzatura
Il data center di Agrisian è gestito dalla consorziata IBM, che è al tempo stesso fornitore delle apparecchiature hardware.
Su informativa dei laboratori tecnici di IBM viene data indicazione sugli aggiornamenti 'firmware' da installare dai tecnici specializzati IBM; vengono inoltre effettuate verifiche sistemistiche sugli aggiornamenti di manteinance e di patch in base alle realese del prodotto da installare.

Separazione rotazione dei compiti.
Il presidio operativo è previsto continuativamente (H/24) da un command center specializzato gestito in remoto da Vimercate, che tramite strumenti e console ha il governo e controllo operativo sull'intero datacenter.
E' prevista inoltre la reperbilità (H/24) per il personale tecnico specializzato, per interventi di secondo livello (di tipo sistemistico) per ognuno degli ambienti gestiti (AIX, Linux, Microsoft, Oracle, ecc.).
E' prevista inoltre assistenza on site in base a turni (per il periodo 07:00 – 20:00) di personale specializzato (sistemisti di secondo livello) per ognuno degli ambienti gestiti (AIX, Linux, Microsoft, Oracle, ecc.).

Attività degli operatori
La conduzione operativa del datacenter viene effettuata tramite l'ausilio di documentazione tecnica fornita dai tecnici specializzati in fase di set up o in successive release.
E' inoltre previsto una comunicazione tra le varie turnazioni per la gestione delle fasi operative, gestita in base ai database interni IBM (siti documentali) nel quale ciascun operatore documenta la propria attività nel corso del turno.

Programmazione ed esecuzione del lavoro.
Tutte le informazioni relative alle attività dei sistemi sono registrate e conservate nel database del prodotto Tivoli, utilizzato per il monitoring dei sistemi del datacenter.

Per la parte relative alle procedure operative (procedure batch), tutte le esecuzioni ed esiti sono registrate e conservate su appositi file di log (uno per ogni settore di competenza).

Controllo delle attività
Il controllo delle elaborazioni o delle modifiche apportate alle basi dati sono gestite sono gestite tramite il tool DOIT4ME.
Le attività batch, di aggiornamento delle basi dati, vengono effettuate tramite l'esecuzione di procedure catalogate, sottoposte a preventivo collaudo e rilascio in esercizio. Il controllo dell'esito avviene mediante verifica dei file di log.

Controllo dei luoghi d archiviazione
Esiste una procedura di archiviazione su supporto magnetico, che con cadenza settimanale prevede il trasporto dalla sede del Datacenter sito in Roma ad un sito protetto a Fidenza, rispondente a criteri di sicurezza e antintrusione. Per maggiori dettagli si rimanda a quanto riportato nella parte relativa al Back Up ed al Disaster recovery

5.4.13 Controlli Applicativi

Inserimento
I dati inseriti sono sottoposti a controlli e verifica di correttezza e completezza prima di essere inseriti a sistema.
Sono effettuati successivi controlli (manuali) di merito al fine della produzione dei dati di pagamento effettuati da procedure informatiche che segnalano e bloccano l'inserimento di eventuali anomalie

Elaborazione
L'elaborazione dei dati dovrebbe essere sottoposta a controlli operativi. La procedura di gestione delle utenze garantisce che dati vengano aggiunti, rimossi o modificati solo da utenti debitamente autorizzati.

Risultati
Il controllo di merito sull'esito delle procedure viene effettuato dal personale che operativamente gestisce le pratiche.

Dati principali
La procedura di gestione delle utenze garantisce che i dati contenuti nei database vengano trattati esclusivamente dagli utenti preventivamente autorizzati.

5.4.14 Postazioni di lavoro

AGEA ha adottato una procedura formalizzata per la gestione dei personal computer e per il monitoraggio sia del software installato che degli antivirus.
È stato istallato un sistema antivirus centralizzato su un nuovo server predisposto in Agenzia.
L'antivirus centralizzato ha sostituito i precedenti antivirus previsti per le singole macchine in modo individuale. Le impronte virali sono aggiornate in modo automatico.

5.4.15 Imprevisti

Agea possiede un piano di Disaster Recovery, fornito da Agrisian e previsto contrattualmente come riportato in precedenza.
In merito alle procedure di back up si rimanda a quanto riportato nel paragrafo 'Sicurezza di supporti magnetici di backup e dei documenti cartacei originali'.

5.4.16 Criticità riscontrate per l'area "Sicurezza logica dei dati o dei server delle applicazioni"

Nell'ambito delle nostre verifiche non abbiamo riscontrato alcuna criticità nell'area "Sicurezza logica dei dati o dei server delle applicazioni".

5.4.17 Conclusioni

Alla luce delle considerazione suesposte, raccomandiamo di dare seguito, nel corso del triennio 2005 - 2007 all'attività di audit, in relazione alle "Direttive di Sicurezza Informatica", sul sistema, sugli standard e sulle procedure organizzative di Agea, così come pianificato.
Si raccomanda al più presto di designare il nuovo responsabile della funzione sicurezza dei sistemi d'informazione dell'Agenzia, per l'attività di coordinamento e supervisione delle strutture organizzative di Agea e del fornitore di servizi telematici interessate alla sicurezza del sistema IT.

5.4.18 Modello di maturità – Compendio

Nell'eseguire l'incarico di revisione conferitoci per l'organismo pagatore AGEA per l'anno finanziario terminato il 15.10.2005, 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'anno finanziario 2007-2008 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 in data 16 dicembre 2005 di garantire la sicurezza del proprio sistema d'informazione sulla base dei criteri stabiliti della norma internazionalmente riconosciuta denominata BS 7799 (come richiamato al punto 1 di cui sopra).

In applicazione dell'orientamento previsto nel paragrafo 3.2) del richiamato documento, riportiamo di seguito le nostre osservazioni e conclusioni provvisorie valide nel periodo oggetto di analisi compreso tra il 16 ottobre 2004 e il 15 ottobre 2005. Le osservazioni e conclusioni sono state formulate sulla base delle interviste condotte con i responsabili dell'organismo pagatore e della documentazione fornitaci nel corso dell'intervento.

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 di seguito i risultati, le raccomandazioni ed il punteggio di conformità per ciascun dominio della norma internazionale scelta per ciascuna delle tre funzioni dall'organismo pagatore (Autorizzazione, Pagamento e Contabilizzazione).

Autorizzazione	Pagamento	Contabilizzazione

BS 7799

Nome del dominio	Risultato	Raccomandazione	Punteggio di conformità (0-6)
Security policy	Esistono procedure standardizzate, documentate ed ampiamente attuate. Esiste una politica precisa in linea con le altre politiche dell'organizzazione.	Raccomandiamo di migliorare le procedure legate alla misurazione dell'efficacia della politica e dei processi al fine di raggiungere la condizione del miglioramento costante.	3
Organizzazione della Sicurezza	L' organizzazione della sicurezza è definita in base ad una politica chiara e formalizzata e si basa sulla collaborazione attiva con diverse organizzazioni. E' vacante la funzione di Responsabile della sicurezza.	Raccomandiamo di nominare quanto prima un nuovo responsabile per la sicurezza, dal momento che la posizione è attualmente scoperta.	3
Classificazione e controllo dei beni	L'agenzia dispone di policy per la classificazione e il controllo dei beni, ma non viene eseguita un'attività di definizione del livello di sicurezza adeguato al bene e di monitoraggio in base a parametri quantitativi e	Raccomandiamo di predisporre una rete di controlli sulla classificazione e il mantenimento dei beni al fine di ottenere analisi oggettive e qualitative sull'utilizzo e lo stato dei beni	2

	qualitativi.	aziendali.	
Aspetti gestionali del personale	Le politiche relative alla gestione del personale sono chiaramente definite all'interno dell'Organizzazione. Non esiste un monitoraggio diretto da parte della direzione e le responsabilità vengono lasciate ai singoli.	Si consigli di monitorare il processo con indicatori di efficienza.	2
Sicurezza Fisica ed ambientale	La sicurezza fisica ed ambientale viene gestita tramite procedure standardizzate e sono predisposte alcune attività di controllo (presso le strutture degli Outsourcer). Si nota, comunque, una carenza di attività di monitoraggio qualitativo e quantitativo rispetto alla sicurezza fisica e di manutenzione delle macchine e delle attrezzature presso gli uffici dell'Agenzia.	Raccomandiamo di predisporre un'attività sistematica di monitoraggio delle problematiche della sicurezza fisica in modo da incrementare il livello di sicurezza delle macchine e delle attrezzature presso gli uffici dell'Agenzia.	3
Gestione delle comunicazioni e dell'operatività	Esistono procedure per la definizione di responsabilità operative, per il funzionamento, lo sviluppo e la	Raccomandiamo di predisporre procedure per monitorare le prestazioni.	2